VMware vCenter Configuration Manager Administration Guide

vCenter Configuration Manager 5.7

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001187-00

vmware

You can find the most up-to-date technical documentation on the VMware Web site at:
http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

© 2006–2013 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About This Book 9

Getting Started with VCM 11
- **Understanding User Access** 11
  - **Running VCM as Administrator on the Collector** 12
- **Log In to VCM** 12
- **Getting Familiar with the Portal** 13
  - **General Information Bar** 13
  - **Toolbar** 14
  - **Navigation Sliders** 15
- **Customizing VCM for your Environment** 16

Installing and Getting Started with VCM Tools 19
- **Install the VCM Tools Only** 19
- **VCM Import/Export and Content Wizard Tools** 20
  - **Run the Import/Export Tool** 20
  - **Run the Content Wizard to Access Additional Compliance Content** 21
- **Run the Deployment Utility** 21
- **Package Studio** 21
- **Foundation Checker** 22

Configuring VMware Cloud Infrastructure 23
- **Virtual Environments Configuration** 23
  - **Managing Agents Virtual Environments** 24
  - **Managing vCenter Server Instances, Hosts, and Guest Virtual Machines** 24
  - **Managing Instances of vCloud Director and vApp Virtual Machines** 25
  - **Managing vShield Manager Instances** 25
- **Configure Virtual Environments Collections** 25
- **Configure Managing Agent Machines for Virtual Environment Management** 26
  - **Collect Machines Data From the Managing Agent Machines** 26
  - **Set the Trust Status for Managing Agent Machines** 27
  - **Configure HTTPS Bypass Setting for Virtual Environments** 28
  - **Enable Managing Agent Machines for Virtual Environments** 28
- **Obtain the SSL Certificate Thumbprint** 29
- **Configure vCenter Server Data Collections** 29
  - **Add vCenter Server Instances** 30
  - **Configure the vCenter Server Settings** 31
  - **Collect vCenter Server Data** 32
  - **vCenter Server Collection Results** 33
  - **Configure vCenter Server Scheduled Collections** 34
- **Configure vCenter Server Virtual Machine Collections** 35
  - **Collect vCenter Server Virtual Machines Data** 35
  - **Manage vCenter Server Virtual Machines** 36
- **Configure vCloud Director Collections** 37
  - **Add vCloud Director Instances** 37
  - **Configure the vCloud Director Settings** 38
  - **Collect vCloud Director Data** 39
  - **vCloud Director Collection Results** 40
- **Configure vCloud Director vApp Virtual Machines Collections** 41
  - **Network Address Translation and vCloud Director vApp Discovery Rules** 41

Discover vCloud Director vApp Virtual Machines 43
Configure vShield Manager Collections 47
Configure ESX Service Console OS Collections 50
Configure the Collector as an Agent Proxy 51
Configure Virtual Machine Hosts 52
Copy Files to the ESX/ESXi Servers 54
Collect ESX Logs Data 55
Virtualization Collection Results 56
Configure the vSphere Client VCM Plug-In 56
Register the vSphere Client VCM Plug-In 56
Configuring the vSphere Client VCM Plug-In Integration Settings 57
Manage Machines from the vSphere Client 58

Running Compliance for the VMware Cloud Infrastructure 59
Create and Run Virtual Environment Compliance Templates 59
Create Virtual Environment Compliance Rule Groups 60
Create and Test Virtual Environment Compliance Rules 61
Create and Test Virtual Environment Compliance Filters 62
Preview Virtual Environment Compliance Rule Groups 62
Create Virtual Environment Compliance Templates 63
Run Virtual Environment Compliance Templates 64
Create Virtual Environment Compliance Exceptions 65
Resolve Noncompliant Virtual Environments Template Results 66
Enforce Compliance Template Results by Using VCM Actions 66
Manually Enforce Compliance Template Results 67
Create Virtual Environment Compliance Exceptions 67
Configure Alerts and Schedule Virtual Environment Compliance Runs 68
Create Virtual Environment Compliance Alert Rules 69
Create Virtual Environments Compliance Alert Configurations 69
Schedule Virtual Environments Compliance Template Runs 70

Configuring vCenter Operations Manager Integration 73
VCM Registration in vCenter Operations Manager for Integration 73
Configure vCenter Operations Manager Change Events 73
Standards Compliance for vCenter Operations Manager 74
Configure vCenter Operations Manager Standards Compliance 74
Scoring Badges for vCenter Operations Manager Standards Compliance 80

Auditing Security Changes in Your Environment 85

Configuring Windows Machines 87
Configure Windows Machines 87
Verify Available Domains 88
Check the Network Authority 89
Assign Network Authority Accounts 89
Discover Windows Machines 90
License Windows Machines 90
Install the VCM Windows Agent on Your Windows Machines 91
Collect Windows Data 93
Windows Collection Results 94
Getting Started with Windows Custom Information 95
Prerequisites to Collect Windows Custom Information 96
Using PowerShell Scripts for WCI Collections 97
Guidelines in PowerShell Scripting for WCI 98
Challenges in PowerShell Scripting for WCI 98
PowerShell Script Signing Policies 101
Create an Example PowerShell Script for Scheduled Tasks 102

Windows Custom Information Change Management 107
Collecting Windows Custom Information 108
Create Your Own WCI PowerShell Collection Script 108
Verify that Your Custom PowerShell Script is Valid 109
Install PowerShell 110
Collect Windows Custom Information Data 110
Run the Script-Based Collection Filter 111
View Windows Custom Information Job Status Details 112
Windows Custom Information Collection Results 113
Run Windows Custom Information Reports 114
Troubleshooting Custom PowerShell Scripts 115

Configuring Linux, UNIX, and Mac OS X Machines 117
Linux, UNIX, and Mac OS X Machine Management 117
Linux, UNIX, or Mac OS X Installation Credentials 119
Configure Collections from Linux, UNIX, and Mac OS X Machines 120
Configure Installation Delegate Machines to Install Linux, UNIX, and Mac OS X Agents 121
Configure the HTTPS Bypass Setting for Linux Agent Installations 123
Enable Linux, UNIX, and Mac OS X Agent Installation 123
Add and License Linux, UNIX, and Mac OS X Machines for Agent Installation 124
Install the VCM Agent on Linux, UNIX, and Mac OS X Operating Systems 125
Collect Linux, UNIX, and Mac OS X Data 132
Linux, UNIX, and Mac OS X Collection Results 133
Configure Scheduled Linux, UNIX, and Mac OS X Collections 133
Create a Dynamic Machine Group for Linux, UNIX, or Mac OS X Machines 134
Schedule Linux, UNIX, and Mac OS X Collections 135

Patching Managed Machines 137
Patch Assessment and Deployment 137
Prerequisite Tasks and Requirements 138
General Requirements 138
Requirements to Patch Solaris Machines in Single-User Mode 140
Requirements to Patch Managed Machines Without Changing the Run Level 140
Requirements to Patch AIX Machines 141
Manually Patching Managed Machines 141
Getting Started with VCM Manual Patching 143
Getting Started with VCM Manual Patching for Linux and UNIX Managed Machines 143
Getting Started with VCM Manual Patching for Windows Managed Machines 150
Configuring An Automated Patch Deployment Environment 156
Configuring the Patching Repository Machine 158
(Optional) Configuring the Alternate Location Patch Repository Machines 161
Configuring VCM to Work with the Patching Repository and Alternate Locations 162
Deploying Patches with Automated Patch Assessment and Deployment 169
Configure VCM for Automatic Event-Driven Patch Assessment and Deployment 170
Generate a Patch Assessment Template 171
Run a Patch Assessment on Managed Machines 172
Add Exceptions for Patching Managed Machines 172
Configure the VCM Administration Settings 173
Generate a Patch Deployment Mapping 175
Configure VCM for Automatic Scheduled Patch Assessment and Deployment 176
How the Linux and UNIX Patch Staging Works 177
How the Linux and UNIX Patching Job Chain Works 178
How the Deploy Action Works 178
Patch Deployment Wizards 179
Running Patching Reports 180

Running and Enforcing Compliance 181

Running Machine Group Compliance 181
Getting Started with SCAP Compliance 194
Conduct SCAP Compliance Assessments 195

Provisioning Physical or Virtual Machine Operating Systems 199
Operating System Provisioning Components 199
How Operating System Provisioning Works 200
Configure Operating System Provisioning Servers 201
Add Operating System Provisioning Servers 202
Set the Trust Status for Operating System Provisioning Servers 202
Collect Operating System Distributions 203
Discover Provisionable Machines 203
Provision Machines with Operating System Distributions 204
Provision Windows Machines 204
Provision Linux Machines 208
Change Agent Communication 213
Provisioned Machines Results 213
Reprovision Machines 214

Provisioning Software on Managed Machines 217
Using Package Studio to Create Software Packages and Publish to Repositories 217
Software Repository for Windows 217
Package Manager for Windows 217
Software Provisioning Component Relationships 218
Install the Software Provisioning Components 218
Install Software Repository for Windows 219
Install Package Studio 220
Install Package Manager on Managed Machines 222
Using Package Studio to Create Software Packages and Publish to Repositories 223
Creating Packages 223
Using VCM Software Provisioning for Windows 225
Collect Package Manager Information from Machines 225
Collect Software Repository Data 226
Add Repository Sources to Package Managers 227
Install Packages 228
Related Software Provisioning Actions 229
Viewing Provisioning Jobs in the Job Manager 230
Create Compliance Rules Based on Software Provisioning Data 230
Create Compliance Rules Containing Software Provisioning Remediation Actions 231

Configuring Active Directory Environments 233
Configure Domain Controllers 233
Verify Available Domains 234
Check the Network Authority Account 234
Assign Network Authority Accounts 235
Discover Domain Controllers 235
License Domain Controllers 236
Install the VCM Windows Agent on Your Domain Controllers 237
Collect Domain Controller Data 238
Configure VCM for Active Directory as an Additional Product 239
Install VCM for Active Directory on the Domain Controllers 240
Run the Determine Forest Action 240
Run the Domain Controller Setup Action 241
Collect Active Directory Data 242
Active Directory Collection Results 242

Configuring Remote Machines 245

VCM Remote Management Workflow 245
Configuring VCM Remote Connection Types 245
Using Certificates With VCM Remote 246
Configure and Install the VCM Remote Client 246
Configure the VCM Remote Settings 246
Install the VCM Remote Client 249
Connect VCM Remote Client Machines to the Network 256
VCM Remote Collection Results 256

Tracking Unmanaged Hardware and Software Asset Data 259
Configure Asset Data Fields 259
Review Available Asset Data Fields 260
Add an Asset Data Field 260
Edit an Asset Data Field 261
Delete a VCM for Assets Data Field 262
Change the Order of Asset Data Columns 262
Refresh Dynamic Asset Data Fields 263
Configure Asset Data Values for VCM Machines 264
Configure Asset Data for Other Hardware Devices 264
Add Other Hardware Devices 265
Add Multiple Similar Other Hardware Devices 265
Edit Asset Data for Other Hardware Devices 265
Edit Asset Data Values for Other Hardware Devices 266
Delete Other Hardware Devices 266
Configure Asset Data for Software 267
Add Software Assets 267
Add Multiple Similar Software Assets 268
Edit Asset Data for Software 269
Edit Asset Data Values for Software 270
Delete Software Data 270

Managing Changes with Service Desk Integration 271
Configure Service Desk Integration 271
View Service Desk Integration in the Console 271
View Service Desk Integration in Job Manager 272

Index 273

About This Book

The *VCM Administration Guide* describes the steps required to configure VCM to collect and manage data from your virtual and physical environment.

Read this document and complete the associated procedures to prepare for a successful implementation of the components.

Intended Audience

This information is written for experienced Windows, Linux, UNIX, or Mac OS X, and virtual environments system administrators who are familiar with managing network users and resources and with performing system maintenance.

To use this information effectively, you must have a basic understanding of how to configure network resources, install software, and administer operating systems. You also need to fully understand your network topology and resource naming conventions.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

VMware VCM Documentation

The vCenter Configuration Manager (VCM) documentation consists of the *VCM Installation Guide*, *VCM Troubleshooting Guide*, VCM online Help, and other associated documentation.

Technical Support and Education Resources

The following technical support resources are available to you. To access the current version of this book and other books, go to http://www.vmware.com/support/pubs.

Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to http://www.vmware.com/support.

Customers with appropriate support contracts should use telephone support for priority 1 issues. Go to http://www.vmware.com/support/phone_support.html.

Support Offerings

To find out how VMware support offerings can help meet your business needs, go to http://www.vmware.com/support/services.

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.

1 Getting Started with VCM

When you use VCM, you must understand user access and how to start VCM from any physical or virtual machine. You must also familiarize yourself with the VCM Web Console features.

This chapter includes the following topics:

Understanding User Access 11
Log In to VCM 12
Getting Familiar with the Portal 13
Customizing VCM for your Environment 16

Understanding User Access

User access determines who has access to VCM and with what roles. To manage your user access, create rules that are assigned to roles. VCM assigns the roles to each user login you create. User access is managed in the Administration User Manager node.

The user account that was used to install VCM is automatically granted access to VCM, placed in the roles of ADMIN and USER, and placed into the Admin role. This user can log in to VCM using the Admin role. The AD_Admin role allows full administration access to AD objects only.

When a user is added to the Admin role in VCM or granted access to the Administration User Manager node, that user is placed in the fixed machine roles Security Administrators and Bulk Insert Administrators Groups. They are also added to the database roles of public, ADMIN, and User in the VCM Database.

Users who will not have access to the Administration User Manager node will be assigned to public. Depending on the functions granted to a user, they might need additional or fewer privileges for their role to function properly.

VCM provides a role named Change Restricted to limit users from making certain changes in your environment. With this role, users can discover machines, collect data from machines, assess machines, display bulletin and template details, check for updates, and view history. Users can add, edit, and delete reports, compliance rules and rule groups, and compliance and patch assessment templates. Users with the Change Restricted role can also install the VCM Agent, upgrade VCM, and uninstall VCM.

When you apply the Change Restricted role to a user's VCM login, they cannot perform the following actions.

- Remote command execution
- Change actions against target managed machines
- Change rollback
- Compliance enforcement
- Patch deployment
- Software deployment
- OS provisioning
- Machine reboots

All VCM user accounts must have the following rights on the VCM Collector machine.

- Ability to log on locally to access IIS
- Read access to the `System32` folder
- Write access to the `CMFiles$\Exported_Reports` folder to export reports
- If default permissions have been changed, read access to the `C:\Program Files (x86)\VMware\VCM\WebConsole` directory and all subdirectories and files

  Users who add machines to VCM using a file or the Available Machines Add Machines action must have write access to `CMFiles$\Discovery_Files`.

Running VCM as Administrator on the Collector

By default for localhost, Internet Explorer on Windows Server 2008 R2 runs with Protected Mode enabled. If you are logged in to VCM as an Administrator, because Protected Mode is enabled, problems can occur with the SQLServer Reporting Service (SSRS) Web service interface components such as dashboards and node summaries.

CAUTION Although you should not access VCM on the Collector using a Web console, to restore the SSRS functionality you can run Internet Explorer as administrator or disable Protected Mode for the zone of the Collector (localhost). If you perform this action, you must take additional precautions to protect the Collector because of the increased exposure to attacks on the Collector through the Web browser, such as cross-site scripting.

Log In to VCM

Access VCM from any physical or virtual machine in your network. The level of access is determined by your VCM administrator.

Prerequisites

- Verify that the physical or virtual machines from which you are accessing VCM have a supported version of Internet Explorer installed. For supported platforms, see the *VCM Installation Guide*.
- Configure the Internet Explorer Pop-up Blocker settings to add your Collector to your list of allowed Web sites, or disable Pop-up Blocker. Click **Internet Explorer** and select **Tools > Pop-up Blocker > Pop-up Blocker Settings** and then add the path for your Collector in the allowable address field.

Procedure

1. To connect to VCM from a physical or virtual machine on your network, open Internet Explorer and type `http://<name-or-IP-address-of-Collector-machine>/VCM`.
2. Type your user network credentials.
3. (Optional) Select **Automatically log on using this role** to have VCM log you in.
4. Click **Log On**.

Your VCM user account can have multiple roles. If you selected the **Automatically log on using this role** option, VCM will automatically log you on as the User Role displayed on the Logon screen. To change roles, you must use the Logoff button in the top right corner of the Console. This action will return you to the Logon screen so that you can use the drop-down menu to select a different role.

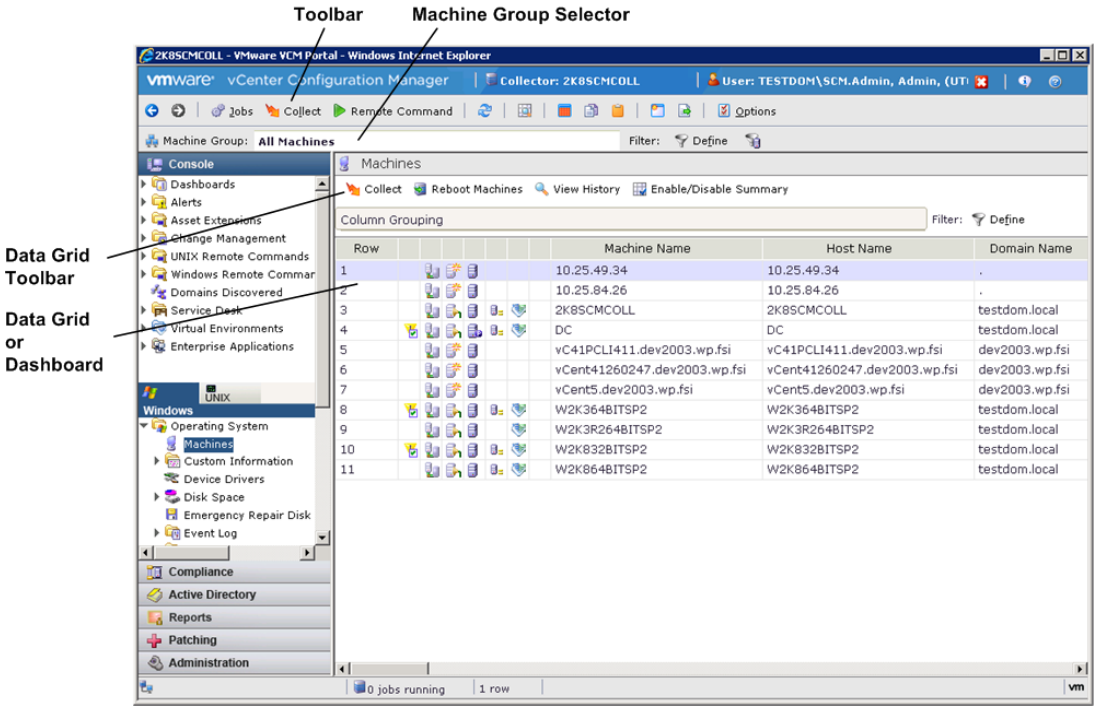
Getting Familiar with the Portal

The VCM Web Console provides access to all VCM features to manage your environment.

The Web Console uses a browser-based interface to run from any Windows machine that has access to the server on which VCM is installed. The Windows machine must be running Internet Explorer or Mozilla Firefox with the Internet Explorer tab plug-in installed.

The Web Console includes several major areas and controls.

Figure 1–1. VCM Portal



General Information Bar

The general information bar displays the VCM Collector's active SQL Server name, your VCM user name and active Role, and the following buttons.

- **Log Out:** Exits the Web Console. The Web Console closes and the VCM Logon screen appears.
- **About:** Displays information about how to contact VMware Technical Support and version information for VCM and all of its components. This information may be important when you contact VMware Technical Support.
- **Help:** Opens the online Help for the currently-active display.

Toolbar

The global toolbar provides you with easily-accessible options to enhance control of your environment and data.

	The left and right arrow buttons navigate to the previous or next page in the data area.
	The Jobs button opens the Jobs Running status window. This button provides access to the Collector status and allows you to stop and restart the Collector service.
	The Collect button opens a wizard that allows you to define and initiate data collections.
	The Remote Commands button allows you to invoke the Remote Commands wizard from the toolbar without having to access the node.
	The Refresh data grid view button refreshes the data grid. Press F5 on the keyboard as an alternative action.
	The View row cells button displays a vertically scrolling view of a single row of data, rather than the table-based data grid view in a separate window, and allows you to move between records.
	The Select all displayed data rows button selects all the rows in the data grid.
	The Copy button copies information from the selected rows in the data grid to the clipboard.
	The Copy link to clipboard button copies the link of the content on-screen to the clipboard.
	The View data grid in separate window button displays the data grid in a separate window.
	The Export displayed data button exports data to a CSV formatted file. This file is exported to `\\<name_of_Collector_machine>\CMfiles$\Exported Reports`.
	The Options button opens the User Options window. These settings pertain to the User who is logged in to VCM. All VCM users can configure these settings to their individual preferences.

Navigation Sliders

The navigation sliders on the left side of the Web Console include the items listed and described in the following table. The individual items that you see in VCM vary depending on the components that you have licensed.

- Active Directory and AD objects based on your role.
- Patching options are available based on your role.
- Administration is visible only to users who have Administrative rights to VCM as part of their VCM role.

For detailed instructions about any of these features, see the online Help.

Slider	Action
Console	■ View, export, or print enterprise-wide, summary information. ■ Review or acknowledge current alert notifications. ■ Manage VCM discovered and non-VCM discovered hardware and software assets. ■ Review changes that occurred from one collection to the next. ■ Create, edit, or run remote commands on a VCM managed Windows or UNIX machine. ■ View information about VCM discovered domains. ■ Navigate and manage integrated service desk events. ■ Manage virtual machines. ■ View your Windows NT Domain and Active Directory related data. ■ View information for enterprise-level applications. ■ Review non-security related UNIX machine-specific information. ■ Review UNIX security data to ensure consistent security configurations across your environment.
Compliance	■ Create and manage Compliance rule groups and templates based on AD objects or machine group data.

Slider	Action
Active Directory	■ View, export, or print enterprise-wide, summary information for Active Directory objects. ■ Review alert notifications for the selected AD location. ■ Review Active Directory-related changes that occurred from one collection to the next. ■ View collected information about Active Directory objects such as Users, Groups, Contacts, Computers, Printers, Shares, and Organizational Units. ■ Review Active Directory site lists, including Site Links, Site Link Bridges, Subnets, Intersite Transports, Servers, Connections and Licensing. ■ View Active Directory Group Policy Container Settings. ■ View information about Active Directory Domains, DCs, and Trusts. ■ Track and display access control entries and security descriptor data on all collected objects. ■ View Active Directory Schema information.
Reports	■ Run out-of-the-box reports against your collected data. ■ Write your own SQL and SSRS reports using VCM's report wizard.
Patching	■ Review a list of bulletins available to VCM. ■ Create, run, or import VCM Patching templates to display the machines that require the patches described in each bulletin. ■ Monitor VCM Patching jobs. ■ Deploy patches.
Administration	■ Manage basic configuration options for VCM. ■ Establish filters to limit the data you collect from machines in your environment. ■ Review how your VCM licenses are being used. ■ Identify and manage your physical and virtual machines. ■ Manage VCM Logins and Roles. ■ Set options for assessment and deployment. ■ View the status of jobs that are currently running, scheduled to run, or completed. ■ Configure VCM to notify you of certain conditions in your environment.

Customizing VCM for your Environment

Customization of your environment is essential to fine-tune the visibility of configuration information so that the policies you develop and the actions you take are appropriate for your IT infrastructure.

Create a machine group structure that matches the organization of the machines in your environment. With these machine groups, you can manage specific machines in your environment such as all SQL Servers in a particular location. You can apply specific changes or create roles and rules for those machines independently from other machines in your environment. This approach ensures that you can restrict access to critical machines to the appropriate users with rights to VCM.

You can customize the following options for your environment.

- **Alerts:** Define the objects and types of changes that you are alerted to when they are detected in VCM. For example, you can set an alert to notify you if a registry setting changes in your environment.
- **Collection Filters and Filter Sets:** Use collection filters to specify the data to collect from the VCM managed machines. A default collection filter is provided for each data type. You can add custom collection filters that are specific to your enterprise. You can apply filters during instant collections and scheduled collections if the filters are included in a filter set. After you create collection filters, organize them into filter sets. You can create specific filter sets or filter set groups for different machine groups. You can apply filter sets during instant collections or scheduled collections.
- **Compliance Templates and Rule Groups:** Use compliance templates and rule groups to define specific settings and verify whether the machines match those criteria. VCM provides prepackaged templates and rules to check the compliance of your machines with regulatory, industry, and vendor standards. VMware provides additional compliance packages that you can import into VCM.
- **Reports:** Create and print tailored reports of information that does not appear in VCM. VCM provides prepackaged reports that you can run after you collect data from your VCM managed machines.
- **Roles and Rules:** VCM roles and access rules work together to control user access to VCM. For example, you can create a role that allows a user to view all data, but not make changes to the environment. You can create a role to run certain reports or a role that allows unlimited access to a single machine group.

  The VCM Change Restricted role limits users from making certain changes in your environment. See "Understanding User Access" on page 11.

Installing and Getting Started with VCM Tools 2

VCM Installation Manager installs several VCM components and tools on the Collector machine during the installation.

This chapter includes the following topics:

Install the VCM Tools Only 19
VCM Import/Export and Content Wizard Tools 20
Run the Deployment Utility 21
Package Studio 21
Foundation Checker 22

Install the VCM Tools Only

You can install the VCM tools on a non-Collector Windows machine.

If you plan to install VCM on the non-Collector Windows machine later, you must uninstall the tools and then install VCM.

Prerequisites

Perform the installation requirements for each tool in the Advanced Installation selection. For example, you can install Import/Export (I/E) and Content Wizard only on a machine that is running VCM.

Procedure

1. On the non-Collector Windows machine on which you want to install the tools, insert the installation CD.
2. In Installation Manager, click **Run Installation Manager**.

   During the installation, follow the installation requirements that Installation Manager reports when Foundation Checker runs.
3. Complete the initial installation pages, and click **Next** on subsequent pages to access the Select Installation Type page.
   a. Clear the **VMware vCenter Configuration Manager** check box.
   b. Select **Tools**.

c. To install a subset of tools, clear the **Tools** check box and select only the individual tools to install.

4. Click **Next**.
5. Complete the remaining instructions and click **Next**.
6. On the Installation Complete page, click **Finish**.
7. On the Installation Manager page, click **Exit**.

VCM Import/Export and Content Wizard Tools

Use the Import/Export Tool and the Content Wizard Tool to move or update VCM business objects. These tools support the migration of any VCM Management Extension for Asset data that was added to VCM manually, but does not import or export any collected data.

The Import/Export Tool supports the following scenarios.

- Back up (export) and restore (import) business objects to the same machine.
- Back up (export) and import (if needed) business objects during a VCM upgrade.
- Export and migrate (import) business objects to additional machines in a multi-Collector environment during setup or to move custom content.
- Use the Content Wizard to download current Compliance Content from VMware and import it into an existing database.
- Using the Command Line Interface, automate the propagation of content to other machines in a multi-collector environment with a "golden machine".
- Aid in disaster recovery by using the Command Line Interface to automate and schedule the backup of VCM content and configuration parameters.

The Command Line Interface (CLI) is a powerful extension of the Import/Export graphic user interface (GUI). In addition to supporting the scenarios noted above, the CLI allows content to be overwritten, as opposed to "rename only", and provides for automation through scripting suitable for customizations.

IMPORTANT Use of the CLI should be restricted to advanced users who exercise caution when testing their scripts.

The Import/Export Tool and Content Wizard Tool were installed on your Collector machine during your VCM installation.

Run the Import/Export Tool

Use the Import/Export Tool to back up your VCM database business objects and import them into a new VCM database or into a recovered VCM database. This tool also supports the migration of any VCM Management Extension for Asset data that was manually added to VCM.

Prerequisites

Install the Import/Export Tool. See "Installing and Getting Started with VCM Tools" on page 19.

Procedure

1. On the Collector, click **Start**.
2. Select **All Programs > VMware vCenter Configuration Manager > Tools > Import Export Tool**.
3. For importing and exporting procedures, click **Help > Contents** and use the online help.

Run the Content Wizard to Access Additional Compliance Content

Use the Content Wizard to import additional VMware content such as VCM Compliance Content Packages. These packages are not available in VCM until you download and import them. Check the VCM Compliance Content Packages to determine if you need to import them.

Prerequisites

Install the Content Wizard. See "Installing and Getting Started with VCM Tools" on page 19.

Procedure

1. On the Collector, click **Start**.
2. Select **All Programs > VMware vCenter Configuration Manager > Tools > Content Wizard Tool**.
3. In the Content Wizard, select **Get Updates from the Internet** and click **Next**.
4. After the wizard identifies available content, click **Next**.
5. Select the updates to install on your Collector and click **Install**.

   When the installation is finished, the Event Log Results window appears.
6. On the Event Log Results window, click **Save** and specify a location to save the logs.
7. Click **Close**.
8. On the Content Wizard page, click **Exit**.

What to do next

View the imported data in VCM. For example, click **Compliance** and select **Machine Group Compliance > Templates**. You can now run any imported compliance template against your collected data.

Run the Deployment Utility

The Deployment Utility for UNIX/Linux and ESX/vSphere copies files to multiple target machines when you configure Linux, UNIX, and ESX/vSphere machines for management in VCM.

Procedure

1. On the Collector, navigate to `C:\Program Files (x86)\VMware\VCM\Tools`.
2. Copy the `DeployUtility-<version>.zip` file from the Collector to your Windows machine.
3. Extract the files.
4. Double-click `DeployUtil.exe` to start the application.

What to do next

In the Deployment Utility, click Help and review the procedure for the type of machine you are configuring.

Package Studio

Use Package Studio to create software packages that can be installed by VCM. It is one component of VCM Software Provisioning that includes the Software Repository for Windows and the Package Manager.

For procedures to run the Package Studio, see the *Software Provisioning Components Installation and User's Guide*.

Foundation Checker

Use the Foundation Checker tool to verify that a Windows machine designated as a VCM Collector meets all of the prerequisites necessary to install VCM.

Installation Manager uses VCM Foundation Checker to check a machine's viability for a successful VCM deployment. Foundation Checker runs system checks that determine various conditions, settings, and requirements, and displays a results file that displays the system checks that passed, failed, or generated warnings.

If the checks run without error, you can install VCM. If the checks identify missing components or incorrect configurations, Foundation Checker instructs you where to verify the component or configuration and how to remedy the errors.

To run the Foundation Checker on a Windows machine on which you will install another instance of VCM, see the *Foundation Checker User's Guide*.

Configuring VMware Cloud Infrastructure 3

VCM collects information from your instances of vCenter Server, vCloud Director, and vShield Manager so that you can then use the information to manage and maintain your virtual environment.

The collected data appears in the Console under the Virtual Environments node. The information is organized in logical groupings based on the information sources, including vCenter Server, vCloud Director, and vShield Manager.

Based on the collected virtual environments data, you can manage the objects and data at an enterprise and individual level, including running compliance rules and reports; running actions, such as changing settings and taking virtual machine snapshots; and managing the guest operating systems as fully managed VCM machines.

This chapter includes the following topics:

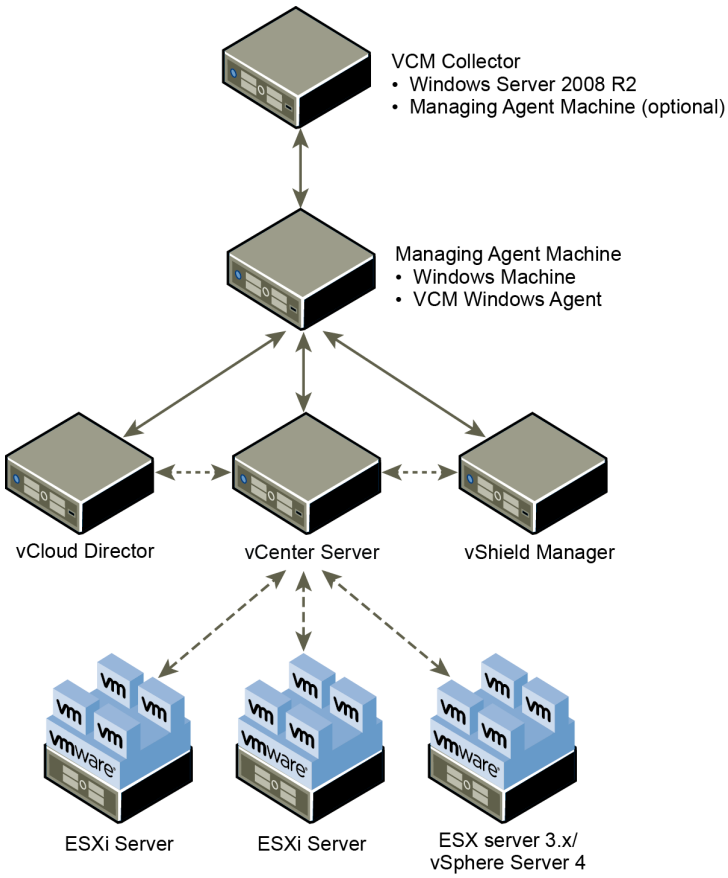
Virtual Environments Configuration 23
Configure Virtual Environments Collections 25
Configure Managing Agent Machines for Virtual Environment Management 26
Obtain the SSL Certificate Thumbprint 29
Configure vCenter Server Data Collections 29
Configure vCenter Server Virtual Machine Collections 35
Configure vCloud Director Collections 37
Configure vCloud Director vApp Virtual Machines Collections 41
Configure vShield Manager Collections 47
Configure ESX Service Console OS Collections 50
Configure the vSphere Client VCM Plug-In 56

Virtual Environments Configuration

To manage your virtual environments, you collect vCenter Server, vCloud Director, and vShield Manager data. To collect the data, you use one or more Managing Agent machines.

After configuring your Managing Agent machines, you add and configure your vCenter Server, vCloud Director, and vShield Manager instances in VCM to use the Managing Agent for communication. For a diagram illustrating how the components are configured together, see Figure 3–1. Virtual Environments Configuration Diagram.

Figure 3–1. Virtual Environments Configuration Diagram



Managing Agents Virtual Environments

The Managing Agent machines must have the 5.5 Agent or later installed. They must also be configured to manage the secure communication between the vCenter Server, vCloud Director, and vShield Manager instances and the Collector. Depending on the size of your Cloud Infrastructure environment, you can use your Collector as a Managing Agent or you can use another Windows machine. If your individual vCenter Server instances manage no more than 1–30 hosts and a maximum of 1000 guests, then you can use the Collector as your Managing Agent. If any of your vCenter Server instances exceed this amount, you must use a Windows machine that is not your Collector as a Managing Agent.

CAUTION Do not use the Windows machines on which your vCenter Server instances are running as Managing Agent machines.

Managing vCenter Server Instances, Hosts, and Guest Virtual Machines

You collect data from vCenter Server instances regarding resources managed by the vCenter Server, and to identify and manage the host and guest machines. The host and guest machines are managed based on configured vCenter Server instances. From VCM, you can run vCenter Server actions such as configuring settings, turning the power on and off, or taking a snapshot. To fully manage the guest machines, install the VCM Agent on the virtual machines and manage their operating system.

Managing Instances of vCloud Director and vApp Virtual Machines

You collect data from vCloud Director instances regarding their configurations, resources managed by vCloud Director, and to identify and manage the vApp virtual machine guest operating systems. To fully manage the guest machines, you install the VCM Agent on the virtual machines and manage their operating system.

Managing vShield Manager Instances

You collect from vShield Manager instances to gather data regarding vShield App security groups. You can run reports on the collected data.

Configure Virtual Environments Collections

To manage your virtual environments, configure your Managing Agent and then implement the procedures that suit your environment.

Procedure

1. "Configure Managing Agent Machines for Virtual Environment Management" on page 26

   The Managing Agents are one or more physical or virtual machines running a supported Windows operating system that manages the communication between the Collector and your instances of vCenter Server, vCloud Director, and vShield Manager.

2. "Obtain the SSL Certificate Thumbprint" on page 29

   When configuring the settings for your virtual environments systems, you can use an SSL certificate thumbprint file to ensure secure communication between the Collector and your instances of vCenter Server, vCloud Director, and vShield Manager.

3. "Configure vCenter Server Data Collections" on page 29

   Collect data from your vCenter Server so that you can identify and manage your virtual environments, including ESX and ESXi hosts, and guest virtual machines.

4. "Configure vCenter Server Virtual Machine Collections" on page 35

   Configure virtual machine collections so that you can identify and manage the guest operating systems on the vCenter Server virtual machines.

5. "Configure vCloud Director Collections" on page 37

   Configure collections from your vCloud Director instances so that you can run compliance and reports, and identify your vApp virtual machines.

6. "Configure vCloud Director vApp Virtual Machines Collections" on page 41

   Collect vCloud Director data so that you can identify and manage the guest operating systems of the vApp virtual machines.

7. "Configure vShield Manager Collections" on page 47

   Configure collections from your vShield Manager instances so that you can run reports on the collected data.

8. "Configure ESX Service Console OS Collections" on page 50

   The ESX Service Console OS Linux data type data and the ESX logs are collected directly from the ESX operating systems, not from vCenter Server. Configure the ESX servers so that you can collect the

Linux data type and ESX log data from the ESX service console operating system.

9. "Configure the vSphere Client VCM Plug-In" on page 56

   The vSphere Client VCM Plug-In provides contextual access to VCM change, compliance, and management functions. It also provides direct access to collected vCenter Server, virtual machine host, and virtual machine guest data.

Configure Managing Agent Machines for Virtual Environment Management

The Managing Agents are one or more physical or virtual machines running a supported Windows operating system that manages the communication between the Collector and your instances of vCenter Server, vCloud Director, and vShield Manager.

The Managing Agent machines must have the 5.5 Agent or later installed. They must also be configured to manage the secure communication between the vCenter Server, vCloud Director, and vShield Manager instances and the Collector. Depending on the size of your Cloud Infrastructure environment, you can use your Collector as a Managing Agent or you can use another Windows machine. If your individual vCenter Server instances manage no more than 1–30 hosts and a maximum of 1000 guests, then you can use the Collector as your Managing Agent. If any of your vCenter Server instances exceed this amount, you must use a Windows machine that is not your Collector as a Managing Agent.

CAUTION Do not use the Windows machines on which your vCenter Server instances are running as Managing Agent machines.

Procedure

1. "Collect Machines Data From the Managing Agent Machines" on page 26

   Collect data from your Managing Agent machines to ensure that VCM identifies the Windows machines as licensed and that the 5.5 Agent or later is installed.

2. "Set the Trust Status for Managing Agent Machines" on page 27

   You can set the trusted status on machines where you have verified that the connection is legitimate. When you set the trust status, you are marking the Agent certificate as trusted.

3. "Configure HTTPS Bypass Setting for Virtual Environments " on page 28

   If your Collector is not configured to use HTTPS, you must configure the Collector to allow HTTP communication when entering sensitive parameter values.

4. "Enable Managing Agent Machines for Virtual Environments" on page 28

   Managing Agent machines must be enabled to perform the necessary communication with your instances of vCenter Server, vCloud Director, and vShield Manager.

Collect Machines Data From the Managing Agent Machines

Collect data from your Managing Agent machines to ensure that VCM identifies the Windows machines as licensed and that the 5.5 Agent or later is installed.

The Managing Agent is the Agent used to collect data from your instances of vCenter Server, vCloud Director and vShield Manager.

Prerequisites

Verify that the Windows machine that you designated as the Managing Agent is licensed and that it has the VCM Agent 5.5 or later installed. See "Configure Windows Machines" on page 87.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed Windows Machines**.
3. Select the target machines and click **Collect** on the VCM toolbar.
4. Select **Machine Data** and click **OK**.
5. Verify that the Selected list includes the target machines and click **Next**.
6. Expand the **Windows** tree, select **Machines**, and click **Next**.
7. Resolve any conflicts and click **Finish**.

What to do next

- When the job is finished, verify that the Agent Version value in the data grid is 5.5 or later.
- Configure the trust status for the Managing Agents. See "Set the Trust Status for Managing Agent Machines" on page 27.

Set the Trust Status for Managing Agent Machines

You can set the trusted status on machines where you have verified that the connection is legitimate. When you set the trust status, you are marking the Agent certificate as trusted.

When you transmit sensitive information, such as credentials, between the Collector and virtual or physical machines on which the Managing Agent is installed, the Agent certificate, including the Agent certificate on the Collector, must be trusted.

If you do not use this level of security, you can set the `Allow sensitive parameters to be passed to agents not verified as Trusted` option to `Yes`. To override the setting, click **Administration** and select **Settings > General Settings > Collector**.

Prerequisites

Ensure that you collected the Machines data type from the Windows machines you are using as Managing Agents. See "Collect Machines Data From the Managing Agent Machines" on page 26.

Procedure

1. Click **Administration**.
2. Select **Certificates**.
3. Select the target machines and click **Change Trust Status**.
4. Add any additional machines to trust to the lower data grid.
5. Select **Check to trust or uncheck to untrust the selected machines** and click **Next**.
6. Review the number of machines affected and click **Finish**.

What to do next

- If your Collector is not configured to use HTTPS, set the HTTPS bypass. See "Configure HTTPS Bypass Setting for Virtual Environments " on page 28.
- Identify the Windows machines as Managing Agents. See "Enable Managing Agent Machines for Virtual Environments" on page 28.

Configure HTTPS Bypass Setting for Virtual Environments

If your Collector is not configured to use HTTPS, you must configure the Collector to allow HTTP communication when entering sensitive parameter values.

If your Collector is configured to use HTTPS, you do not need to modify this setting.

Procedure

1. Click **Administration**.
2. Select **Settings > General Settings > Collector**.
3. Select **Allow HTTP communication (HTTPS bypass) when entering sensitive parameter values** and click **Edit Settings**.
4. Select **Yes** and click **Next**.
5. Review the summary and click **Finish**.

What to do next

Identify the Windows machines as Managing Agents. See "Enable Managing Agent Machines for Virtual Environments" on page 28.

Enable Managing Agent Machines for Virtual Environments

Managing Agent machines must be enabled to perform the necessary communication with your instances of vCenter Server, vCloud Director, and vShield Manager.

Prerequisites

- Ensure that the Managing Agent machines are trusted machines. See "Set the Trust Status for Managing Agent Machines" on page 27.
- If your Collector is not configured to use HTTPS, set the HTTPS bypass. See "Configure HTTPS Bypass Setting for Virtual Environments " on page 28.

Procedure

1. Click **Administration**.
2. Select **Administration > Machines Manager > Licensed Machines > Licensed Windows Machines**.
3. Select the Managing Agent machines and click **Change Managing Agent Status**.
4. Add any additional machines to the lower data grid.
5. Select **Enable - allow the selected machines to be used as managing agents** and click **Next**.
6. Review the number of machines affected and click **Finish**.

What to do next

- To maintain secure communication, you need the SSL certificates from your instances of vCenter Server, vCloud Director, and vShield Manager. See "Obtain the SSL Certificate Thumbprint" on page 29.
- Configure the collections from your instances of vCenter Server, vCloud Director, and vShield Manager.
  - See "Configure vCenter Server Data Collections" on page 29.
  - See "Configure vCloud Director Collections" on page 37.
  - See "Configure vShield Manager Collections" on page 47.

Obtain the SSL Certificate Thumbprint

When configuring the settings for your virtual environments systems, you can use an SSL certificate thumbprint file to ensure secure communication between the Collector and your instances of vCenter Server, vCloud Director, and vShield Manager.

You can use this procedure to copy and save the thumbprint in advance of configuring the settings, or you can follow the process while you are using the wizard.

This procedure applies when your certificates are not properly trusted. If your certificates are configured and trusted, you must log onto the target machine to retrieve the thumbprint from the certificate store.

Prerequisites

Ensure that you have network access to the target instances of vCenter Server, vCloud Director, and vShield Manager from which you need the thumbprint string.

Procedure

1. Open Internet Explorer.
2. In the address bar, type `https://<your vcenter server, vcloud director, or vshield manager instance>`.
3. On the certificate error page, click **Continue to this website**.
4. On the address bar, click **Certificate Error** and select **View Certificates**.
5. Click the **Details** tab.
6. In the list, select **Thumbprint**.
7. Copy the thumbprint string to your clipboard or to a file so that you can access it when needed.

Configure vCenter Server Data Collections

Collect data from your vCenter Server so that you can identify and manage your virtual environments, including ESX and ESXi hosts, and guest virtual machines.

Prerequisites

- Configure your Managing Agent machines. See "Configure Managing Agent Machines for Virtual Environment Management" on page 26.
- To maintain secure communication, you need the SSL certificates from your instances of vCenter Server. See "Obtain the SSL Certificate Thumbprint" on page 29.

Procedure

1. "Add vCenter Server Instances" on page 30

   Add the vCenter Server instances to VCM so that you can license and collect vCenter Server data using the Managing Agent.

2. "Configure the vCenter Server Settings" on page 31

   Configure the Managing Agent, communication, and vCenter Server access options so that VCM can collect host and guest data from the vCenter Server instances.

3. "Collect vCenter Server Data" on page 32

   Collect the vCenter Server, host, and guest data from the vCenter Server instances. The data is displayed by detailed data type and appears in the VCM Console.

The collectedvCenter Server data appears in the Console in the Virtual Environments node. The collected vCenter Server data helps you identify and manage vCenter Server, host, and guest objects. See " vCenter Server Collection Results" on page 33.

Add vCenter Server Instances

Add the vCenter Server instances to VCM so that you can license and collect vCenter Server data using the Managing Agent.

In addition to adding the vCenter Server instances, and you can also add the Windows machine on which the vCenter Server is installed and manage the underlying Windows operating system.

Prerequisites

Know the names and domain information for the vCenter Server instances in your environment.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Available Machines**.
3. Click **Add Machines**.
4. On the Add Machines page, select **Basic: Name, Domain, Type**, **Automatically license machines**, and click **Next**.
5. On the Manually Add Machines - Basic page, configure these options to identify the vCenter Server instances.

Option	Description
Machine	Name of the vCenter Server.
Domain	Domain to which the vCenter Server belongs.
Type	Domain type.
Machine Type	Select vCenter (Windows).

6. Click **Add**.

The machine information is added to the list.

7. (Optional) Add other vCenter Server instances as needed.
8. When all your vCenter Server are added to the list, click **Next**.
9. On the Information page, review the summary and click **Finish**.

What to do next

- Configure the vCenter Server settings. See "Configure the vCenter Server Settings" on page 31.
- Manage the Windows operating systems on which vCenter Server instances are running. See "Configure Windows Machines" on page 87.

Configure the vCenter Server Settings

Configure the Managing Agent, communication, and vCenter Server access options so that VCM can collect host and guest data from the vCenter Server instances.

Prerequisites

- Collect Machines data from the Windows machine that you designated as your Managing Agent. See "Collect Machines Data From the Managing Agent Machines" on page 26.
- If you are using SSL Certificates to maintain secure communication, you must provide the certificate thumbprint from the target system when configuring the settings. See "Obtain the SSL Certificate Thumbprint" on page 29.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed Virtual Environments**.
3. Select the vCenter Server instances and click **Configure Settings**.
4. On the Virtual Environment page, verify that the vCenter Server instances appear in the lower pane and click **Next**.

5. On the Managing Agent and Communication Settings page, configure the settings that are applied to all selected vCenter Server instances and click **Next**.

Option	Description
Managing Agent	Select the Windows machine to manage communication between the Collector and the vCenter Server instances. This Windows machine must have the 5.5 Agent or later installed. You can use the Collector as your managing agent.
Port	Type the port used by the VMware Infrastructure SDK on the vCenter Server instances. The default value is 443.
User ID	Type a vCenter Server instance user name. The user must have a vCenter Server administrative role or an unrestricted read only role.
Password	Type the password for the vCenter Server instance user ID.
Confirm Password	Type the password again.
Ignore untrusted SSL Certificate	Select one of the following certificate options. ■ Yes: Ignores the requirement for a valid signed certificate. ■ No: Requires a valid signed certificate.

6. If you selected No on the Managing Agent and Communication Settings page, you must type or paste the thumbprint string in the text box and click **Next**.
7. On the Important page, click **Finish**.

What to do next

Collect vCenter Server data. See "Collect vCenter Server Data" on page 32.

Collect vCenter Server Data

Collect the vCenter Server, host, and guest data from the vCenter Server instances. The data is displayed by detailed data type and appears in the VCM Console.

Prerequisites

Configure the vCenter Server settings. See "Configure the vCenter Server Settings" on page 31.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed Virtual Environments**.
3. Select the vCenter Server instances and click **Collect** on the VCM toolbar.
4. On the Collection Type page, select **Machine Data** and click **OK**.
5. On the Machines page, verify that the Selected list includes all the vCenter Server instances from which you are collecting and click **Next**.
6. On the Data Types page, select the Virtualization vCenter Server data types that you want to collect from the vCenter Server instances and click **Next**.
7. On the Important page, resolve any conflicts and click **Finish**.

What to do next

- Review the collected virtualization data. Click **Console** and select **Virtual Environments > vCenter**.
- (Optional) Schedule vCenter Server collections. See "Configure vCenter Server Scheduled Collections" on page 34.

vCenter Server Collection Results

The collectedvCenter Server data appears in the Console in the Virtual Environments node. The collected vCenter Server data helps you identify and manage vCenter Server, host, and guest objects.

Option	Description
Console	View the Virtual Environments dashboards. Click Click **Console** and select **Dashboards > Virtual Environments**. View the collected vCenter Server data. Click **Console** and select **Virtual Environments > vCenter** to access the collected data. View the change logs for the virtual environments. Click **Console** and select **Change Management** to access the collected data.
Compliance	Access compliance rules that you create based on the collected vCenter Server data using the Virtual Environment Compliance node. You cannot create enforceable compliance rules for vCenter Server data. The compliance rules for the virtual machines you license and on which you install the Agent are managed in the Machine Group Compliance node.
Reports	Run configured Virtual Environments reports, including a vCenter Summary report. Click **Reports** and select **Machine Group Reports > Virtual Environments**. Create reports based collected vCloud Director objects. Click **Reports** and select **Virtual Object Reports**.
Administration	Displays managed vCenter Server instances from which you are collecting data. Click **Administration** and select **Machines Manager > Licensed Machines > Licensed Virtual Environments** to view licensed vCenter Server instances.
Administration > Machine Groups	Dynamic machine groups based on vCenter Server objects. These objects include instances, hosts, and guest machines, and are used to limit the displayed data.

Configure vCenter Server Scheduled Collections

Configure VCM to regularly collect vCenter Server data from your vCenter Server machine groups to ensure that you are using current results when you are viewing the data and when running reports or compliance.

This action is not required, but scheduling your collections improves your configuration management efficiency.

Procedure

1. "Create vCenter Server Machine Groups" on page 34

   Create a Windows machine group that contains your vCenter Server instances so that you can run collections on the member machines.

2. "Schedule vCenter Server Collections" on page 34

   Schedule the collection job to run against your vCenter Server machine group with the the Default filter set applied so that you regularly collect the vCenter Server and Windows data from the vCenter Server instances.

Create vCenter Server Machine Groups

Create a Windows machine group that contains your vCenter Server instances so that you can run collections on the member machines.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Machine/Virtual Object Groups > All Windows Machines**.
3. Click **Add Group**.
4. Type the name and description of the machine group and click **Next**.

   For example, type the name vCenter Server Instances.

5. Select **Static** and click **Next**.
6. Add the Windows machines that are running vCenter Server to the Selected list and click **Next**.
7. Click **Finish**.

   The group is added to the All Windows Machines list.

What to do next

Schedule the collection of the vCenter Server data types from the vCenter Server instances. See "Schedule vCenter Server Collections" on page 34.

Schedule vCenter Server Collections

Schedule the collection job to run against your vCenter Server machine group with the the Default filter set applied so that you regularly collect the vCenter Server and Windows data from the vCenter Server instances.

Prerequisites

Create a Windows machine groups that includes the machines that are running vCenter Server. See "Create vCenter Server Machine Groups" on page 34.

Procedure

1. Click **Administration**.
2. Select **Job Manager > Scheduled**.
3. Click **Add**.
4. Select **Collection** and click **Next**.
5. Type a job name and description and click **Next**.

   For example, vCenter Server Collections.
6. Select **Default** filter set and click **Next**.
7. Select your vCenter Server machine group and click **Next**.

   For example, vCenter Server Instances.
8. Configure when the collection job runs and click **Next**.

   For example, every four hours starting today.
9. Resolve any conflicts and click **Finish**.

   The collection job is added to your Scheduled Jobs list.

What to do next

After a scheduled run time, verify that the job ran. The information is available in Job Manager history for scheduled collections. Select the time and review the general status and success. View the machine detail status if the collection was not 100% successful.

Configure vCenter Server Virtual Machine Collections

Configure virtual machine collections so that you can identify and manage the guest operating systems on the vCenter Server virtual machines.

VCM manages virtual machines as guest machines and as Windows, Linux, or UNIX machines. To manage the virtual machines as guest machines, you collect vCenter Guests data from your vCenter Server. To manage the virtual machines based on operating system, you license, install the VCM Agent, and collect data directly from the managed machines.

You can identify the virtual machines in your environment two ways.

- Collect vCenter Guests data from you vCenter Servers and manage the virtual Windows, Linux, or UNIX machines. See "Collect vCenter Server Virtual Machines Data" on page 35.
- Manually discover Windows Machines or add Linux or UNIX machines. For Windows machines, see "Discover Windows Machines" on page 90. For Linux or UNIX machines, see "Configure Collections from Linux, UNIX, and Mac OS X Machines" on page 120.

Collect vCenter Server Virtual Machines Data

Identify and license your virtual machines that are identified based on collected vCenter Guests data.

Prerequisites

Manage your vCenter Servers in VCM. See "Configure vCenter Server Data Collections" on page 29.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Available Machines > Licensed Virtual Environments**.
3. Select the vCenter Servers and click **Collect** on the VCM toolbar.
4. On the Collection Type page, select **Machine Data** and click **OK**.
5. On the Machines page, verify that the Selected list includes all the vCenter Servers from which you are collecting and click **Next**.
6. On the Data Types page select **Virtualization > vCenter Guests** and click **Next**.
7. On the Important page, resolve any conflicts and click **Finish**.

What to do next

License your virtual machines. See "Manage vCenter Server Virtual Machines " on page 36.

Manage vCenter Server Virtual Machines

Add and license the virtual machines identified based on a vCenter Guests collection from your vCenter Servers. If you are managing Windows virtual machines, you can also install the VCM Agent.

Using the Manage Guests wizard, you can add the virtual machines to the appropriate Available Machines data grid based on operating system, license the virtual machine based on operating system, or, for Windows machines, license and install the Agent.

Prerequisites

Collect vCenter Guests data from your vCenter Servers. See "Collect vCenter Server Virtual Machines Data" on page 35.

Procedure

1. Click **Console**.
2. Select **Virtual Environments > vCenter > Guests > Summary**.
3. Select either your Windows virtual machines or your Linux or UNIX virtual machines and click **Manage Guests**.
4. On the Default Domain page, configure the options and click **Next**.
   a. Specify the Domain in which the machines are running.
   b. Select the Domain Type.
5. On the Edit VM Guest Machine Info page, review the list and update or remove virtual machines, and click **Next**.
6. On the License VM Guests page, configure the options and click **Next**.
   a. Select **License the selected machines**.
   b. (Windows machines only) Select **Install VCM agents for the selected Windows machines**, and click **Next**.
7. On the Confirm Your Changes page, review the changes and click **Finish**.

What to do next

- For Windows operating system guest machines on which you installed the Agent, collect from the Windows virtual machines. See "Collect Windows Data" on page 93. If you did not install the Agent, see "Install the VCM Windows Agent on Your Windows Machines" on page 91.
- For Linux or UNIX operating system guest machines you must install the Agent. See "Configure Collections from Linux, UNIX, and Mac OS X Machines" on page 120.

Configure vCloud Director Collections

Configure collections from your vCloud Director instances so that you can run compliance and reports, and identify your vApp virtual machines.

Prerequisites

- Configure your Managing Agent machines. See "Configure Managing Agent Machines for Virtual Environment Management" on page 26.
- To maintain secure communication, you need the SSL certificates from your instances of vCloud Director. See "Obtain the SSL Certificate Thumbprint" on page 29.

Procedure

1. "Add vCloud Director Instances" on page 37

   Add the instances of vCloud Director to VCM so that you can license and collect vCloud Director data using the Managing Agent.

2. "Configure the vCloud Director Settings" on page 38

   Configure the Managing Agent, communication, and vCloud Director access options so that VCM can collect virtual machine data from your instances of vCloud Director.

3. "Collect vCloud Director Data" on page 39

   Collect the data from the instances of vCloud Director. The data is displayed by detailed data type and appears in the VCM Console.

The collected vCloud Director data appears in the Console in the Virtual Environments node. The data helps you identify and manage vApp virtual machines. See "vCloud Director Collection Results" on page 40.

Add vCloud Director Instances

Add the instances of vCloud Director to VCM so that you can license and collect vCloud Director data using the Managing Agent.

In addition to adding the instances of vCloud Director, and you can also add the Red Hat machine on which the vCloud Director instance is installed and manage the underlying Red Hat operating system.

Prerequisites

Know the names and domain information for the instances of vCloud Director in your environment.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Available Machines**.
3. Click **Add Machines**.
4. On the Add Machines page, select **Basic: Name, Domain, Type**, **Automatically license machines**, and click **Next**.
5. On the Manually Add Machines - Basic page, configure these options to identify the instances of vCloud Director.

Option	Description
Machine	Name of the vCloud Director instance.
Domain	Domain to which the vCloud Director instance belongs.
Type	Domain type.
Machine Type	Select vCloud Director.

6. Click **Add**.

   The machine information is added to the list.
7. (Optional) Add other instances of vCloud Director as needed.
8. When all your instances of vCloud Director are added to the list, click **Next**.
9. On the Information page, review the summary and click **Finish**.

What to do next

- Configure the vCloud Director settings. See "Configure the vCloud Director Settings" on page 38.
- Manage the Red Hat operating systems on which your vCloud Director instances are running. See "Configure Collections from Linux, UNIX, and Mac OS X Machines" on page 120.

Configure the vCloud Director Settings

Configure the Managing Agent, communication, and vCloud Director access options so that VCM can collect virtual machine data from your instances of vCloud Director.

Prerequisites

- Collect Machines data from the Windows machine that you designated as your Managing Agent. See "Collect Machines Data From the Managing Agent Machines" on page 26.
- If you are using SSL Certificates to maintain secure communication, you must provide the certificate thumbprint from the target system when configuring the settings. See "Obtain the SSL Certificate Thumbprint" on page 29.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed Virtual Environments**.
3. Select the vCloud Director instances and click **Configure Settings**.
4. On the Virtual Environment page, verify that the vCloud Director instances appear in the lower pane and click **Next**.
5. On the Managing Agent and Communication Settings page, configure the settings that are applied to all selected vCloud Director instances and click **Next**.

Option	Description
Managing Agent	Select the Windows machine to manage communication between the Collector and the vCloud Director instances. This Windows machine must have the 5.5 Agent or later installed. You can use the Collector as your managing agent.
Port	Type the port used by the API on the vCloud Director instance. The default value is 443.
User ID	Type a vCloud Director instance user name. The user must have a vCloud Director administrative role or an unrestricted read only role. Use a full vCloud Director administrative user, such as administrator@system.
Password	Type the password for the vCloud Director instance user ID.
Confirm Password	Type the password again.
Ignore untrusted SSL Certificate	Select one of the following certificate options. ■ Yes: Ignores the requirement for a valid signed certificate. ■ No: Requires a valid signed certificate.

6. If you selected No on the Managing Agent and Communication Settings page, you must type or paste the thumbprint string in the text box and click **Next**.
7. On the Important page, click **Finish**.

What to do next

Collect vCloud Director data. See "Collect vCloud Director Data" on page 39.

Collect vCloud Director Data

Collect the data from the instances of vCloud Director. The data is displayed by detailed data type and appears in the VCM Console.

Prerequisites

Configure the vCloud Director settings. See "Configure the vCloud Director Settings" on page 38.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed Virtual Environments**.
3. Select the vCloud Director instances and click **Collect** on the VCM toolbar.
4. On the Collection Type page, select **Machine Data** and click **OK**.
5. On the Machines page, verify that the Selected list includes all the vCloud Director instances from which you are collecting and click **Next**.
6. On the Data Types page, select the Virtualization vCloud Director data type that you want to collect from the vCloud Director instances and click **Next**.
7. On the Important page, resolve any conflicts and click **Finish**.

What to do next

Review the collected virtualization data. Click **Console** and select **Virtual Environments > vCloud Director**.

Discover the vApp virtual machines created by the vCloud Director and make them available in VCM. See "Discover vCloud Director vApp Virtual Machines" on page 43.

vCloud Director Collection Results

The collected vCloud Director data appears in the Console. The discovered virtual machines appear on Administration. After you license the virtual machines and install the Agent, you manage them based on their operating system.

The displayed data is only as current as the last time you collected data from your vCloud Director instances and from your managed machines.

Option	Description
Console	View collected vCloud Director instance data. Click **Console** and select**Virtual Environments > vCloud Director**. View the change logs for the virtual environments. Click **Console** and select **Change Management** to access the collected data.
Compliance	Access compliance rules that you create based on the collected vCloud Director data using the Virtual Environment Compliance node. You cannot create enforceable compliance rules for vCloud Director data. The compliance rules for the virtual machines that you license and on which you install the Agent are managed in the Machine Group Compliance node.

Option	Description
Reports	Run a configured vCloud Director report. Click **Reports** and select **Machine Group Reports > Virtual Environments > vCloud Director Managed VMs**. The report includes the vCloud Director Instance, Organization, Organization virtual datacenter, vApp Name, the VC Machine Name, and the related networking data. Create reports based collected vCloud Director objects. Click **Reports** and select **Virtual Object Reports**.
Administration	Displays managed vCloud Director instances from which you are collecting data. Click **Administration** and select **Machines Manager > Licensed Machines > Licensed Virtual Environments**. Displays the discovered virtual machines with a machine name that is based on your configuration options in the discovery rule. For example, OrgName:vAppName:VirtualMachineName. Click **Administration** and select **Machines Manager**. ■ If the machines are not licensed and the Agent is not installed, the machines appear in the Available Machines data grid based on the operating system. ■ If the machines are licensed and the Agent is installed, the machines appear in the Licensed Machines data grid based on the operating system.
Administration > Machine Groups	Dynamic machine groups based on vCloud Director objects, including instances and guest machines, are used to limit the displayed data.

Configure vCloud Director vApp Virtual Machines Collections

Collect vCloud Director data so that you can identify and manage the guest operating systems of the vApp virtual machines.

To accommodate how vCloud Director manages vApps, which can include duplicate names, IP addresses, and MAC addresses, VCM collects and displays internal and external IP address information, internal machine name information, and vCenter machine name information collected directly from vCloud Director. Based on the collected data, you determine how VCM constructs a unique virtual machine name and specify which IP address to use based on the network address translation (NAT) mapping level.

To identify the vCloud Director virtual machines, you configure discovery rules that analyze data collected from the vCloud Director REST API and use the vApp virtual machine information to add new virtual machines to VCM. After installing the Agent and licensing the virtual machines, you manage the new machines based on their operating systems. The machines appear in VCM based on your configured naming convention.

Network Address Translation and vCloud Director vApp Discovery Rules

To configure the connection string when creating a vCloud Director virtual machines discovery rule, you must know how network address translation (NAT) is implemented in your vCloud Director instances.

The vCloud Director administrator configures the NAT mapping. How the virtual machines are configured with NAT and where VCM is in the network determines the connection string that VCM uses to communicate with the virtual machines.

vCloud Director 1.0 and 1.5 support a variety of vApp network configurations. VCM supports these scenarios.

- VCM is located in the vApp with the virtual machines that it is managing.
- The vApp has a direct connection to the org network.
- The vApp has a direct connection to the external network.
- The vApp has a one-to-one IP address NAT connection to the organization network with direct connection to the external network.
- The vApp has a one-to-one IP address NAT connection to the organization network with a one one-to-one IP address NAT connection to the external network.
- The vApp has a direct connection to the organization network with one IP address to one IP address NAT connection to the external network.

VCM does not support one to many IP addresses NAT mapping for vCloud Director vApp virtual machines.

To determine the connection string to use when discovering the vCloud Director virtual machines, you must know where VCM is located in the network and how NAT is implemented.

Table 3–1. Determining the Connection String Based on Network Configuration

Location of VCM or the Proxy Server on the Network	External Network	Organization Network	Discovery Rule Connection String
In the managed vApp	NA	NA	Internal IP
On Org Network	NA	Direct connection.	None (use DNS) or Internal IP
On Org Network	NA	NAT at vApp level.	vApp External IP
On External Network	Direct Connection	Not connected or direct connection.	Internal IP
On External Network	Direct from Organization	NAT at vApp level.	vApp External IP
On External Network	NAT at Org level	The vApp level IP is collected from vCloud Director, but it is not used for the VCM connection.	Org External IP

After you collect the vCloud Director data, you can view the internal and external IP addresses in network information for the virtual machines.

Best Practice

VCM cannot use DCOM to communicate with vCloud Director vApp virtual machines across NAT mapped networks.

In a NAT mapped network environment, your best practice is to install the Agent on the vApp template machines. You must manually install the Agent with the HTTP mode enabled, but you must not collect data from these template machines. Collecting from the template machines generates machine-specific information that will cause the virtual machines created from the template to run incomplete collections.

If you discovered NAT mapped vApp virtual machines that do not have the Agent preinstalled on the templates from which they were created, you must manually install the Agent. The Agent must be installed with the HTTP protocol enabled. See Manually Install the Windows Agent in the online Help.

Discover vCloud Director vApp Virtual Machines

To begin managing the vCloud Director vApp virtual machines, create and run a VCM discovery rule. The rule runs against the collected vCloud Director data in the VCM database.

Prerequisites

- Collect vCloud Director data. You can run the discovery only on the collected data. See "Collect vCloud Director Data" on page 39.
- Determine how NAT is used in your vCloud Director network and where VCM is located in relationship to the network. See "Network Address Translation and vCloud Director vApp Discovery Rules" on page 41.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Discovery Rules**.
3. On the data grid toolbar, click **Add**.
4. On the Discovery Rules page, type a Name and Description, and click **Next**.
5. On the Discovery Method page, select **By DB Discovery** and click **Next**.
6. On the Discovery Query page, in the Discovery Query drop-down menu, select **vCloud Director Managed VMs** and click **Next**.
7. On the Discovery Query Parameters page, configure the options to use when discovering and adding the data to VCM and click **Next**.

Option	Description
Machine Name Format	Select the format used to display the virtual machine name. You can select the vCenter name for the virtual machine or select a combination of names for the virtual machine that includes the vApp that contains the virtual machine, the vCloud Director organization, and the vCloud Director instance. With these formats, you can easily sort, group, and display the data in VCM. The composite name is limited to 128 characters. ■ **VCName:** Name of the virtual machine in vCenter. vCloud Director creates the virtual machine and generates the name of the virtual machine, which includes the machine's host name and the 10-digit identification number of the virtual machine in vCenter. This name is unique in a single vCloud Director instance. ■ **vApp:VCName:** Name of the vApp that contains the virtual machine and the name of the virtual machine in vCenter. ■ **vDC:vApp:VCName:** Name of the virtual datacenter with the vApp name and the name of the virtual machine in vCenter. ■ **Org:vDC:vApp:VCName:** Name of the vCloud Director organization with the virtual datacenter name, the name of the vApp that contains the virtual machine, and the name of the virtual machine in vCenter. ■ **Cloud:Org:vDC:vApp:VCName:** Name of the vCloud Director instance with the name of the vCloud Director organization, the virtual datacenter name, the name of the vApp that contains the virtual machine, and the name of the virtual machine in vCenter.
Machine Name Delimiter	Select a character to separate the elements of the vCloud Director hierarchy that you use as the machine name.
Domain Name	Type or select the domain in which you are managing the virtual machines.
Domain Type	Select the type of domain to which you are adding the virtual machines.
Protocol	Select the protocol by which the Collector will communicate with the Agent. If the virtual machines in the vApp uses NAT mapping, you must select HTTP. If the virtual machines do not use NAT, you can use HTTP or DCOM.
HTTP Port	If you selected the HTTP protocol, you must specify the port used to communicate with the Collector. Uses the HTTP Listener on the target machine. The listener is configured to listen on the designated port. Port 26542 is the default setting. Accepted port values range from 1–65535. Other applications should not use this port.

Option	Description
Use a proxy server	Select **Yes** if you use a proxy server for communication between the Collector and the Agents on the virtual Windows machines. Select **No** if you do not use a proxy server or if you are managing Linux or UNIX machines. If the machines you add are Windows machines, you can select a proxy server for communication between the Collector and the Agents on managed machines that are located on the other side of a proxy server. The proxy server routes requests from the Collector to the Agents on managed machines. A proxy server can only be used with Windows HTTP agents.
Connection String	Select the IP address to use when communicating with the virtual machines. This address can differ from the address that resolves by machine name from DNS or other name resolution systems. Use this address when VCM must contact a vApp virtual machine through a Network Address Translation (NAT) address, or when DNS available to the Collector cannot resolve the vApp virtual machines. If the virtual machines that appear in the console as part of your vCloud Director collections are not added as part of your database discovery of vCloud Director data, ensure that the internal or external connection string is valid for the virtual machines. If the connection string is set to External IP, you will discover only machines with external IP addresses. The connection string depends on the type and level at which NAT mapping is configured. ■ **None (use DNS):** The Collector resolves the IP address to the virtual machine based on the configured name resolution mechanisms. For example, DNS or Hosts. ■ **Internal IP:** The IP address that the virtual machine has in the vApp. ■ **vApp External IP:** The IP address external to the vApp addresses of the virtual machines that are configured with NAT at the vApp level. ■ **Org External IP:** The IP address external to the organization addresses of the virtual machines that are configured with NAT at the organization level or at the organization and vApp level. If NAT is implemented at the vApp and organization level, select this option.
Cloud Name Filter	To run the query against all system resources in a vCloud Director instance, type the name of the vCloud Director instance. SQL wildcard expressions are allowed. Discovers all virtual machines managed by the vCloud Director instance.
Org Name Filter	To run the query against an organization in a vCloud Director instance, type the name of the organization. SQL wildcard expressions are allowed. Discovers all virtual machines in the organization.

Option	Description
vDC Name Filter	To run the query against a virtual datacenter in a vCloud Director instance, type the name of the virtual datacenter. SQL wildcard expressions are allowed. Discovers all virtual machines in the virtual datacenter.
vApp Name Filter	To run the query against a vApp, type the name of the vApp. SQL wildcard expressions are allowed. Discovers all virtual machines in the vApp.
VM Name Filter	To run the query to add a specific virtual machine, type the name of the machine. SQL wildcard expressions are allowed. Discovers the virtual machine.
Network Name Filter	To run the query against resources on a particular network, type the name of the network. SQL wildcard expressions are allowed. Discovers all virtual machines on the network.
IP Address Filter	To run the query to add virtual machines with a particular IP address, type the address. SQL wildcard expressions are allowed. Discovers all virtual machines with that IP address.
Include rule in post collection IP update	Select **Yes** to include the properties of this discovery rule to update the connection string information for the discovered machines when new vCloud Director data is collected. Select **No** to not update the connection string information.

8. On the Important page, select the options and click **Finish**.

Option	Description
Would you like to run this Discovery Rule now?	Select **Yes**.
License and Install Agent on Discovered Machines	If you do not use NAT mapping, select the option to install the Agent. If you use NAT mapping, you must manually install the Agent on the discovered machines.

What to do next

- Review the discovery jobs to determine if your job finished. Click **Administration** and select **Job Manager > History > Other Jobs**.
- Review the collected vCloud Director vApp virtual machine data. Click **Administration** and select **Machines Manager**. In **Available Machines** and **Licensed Machines**, select the operating system type and review the list for the added virtual machines.
- If the discovered machines are listed only in the Available Machines list and the virtual machines use NAT mapping, you must manually install the Agent appropriate for the operating system. See the online Help for the manual installation procedures.

Configure vShield Manager Collections

Configure collections from your vShield Manager instances so that you can run reports on the collected data.

Prerequisites

- Configure your Managing Agent machines. See "Configure Managing Agent Machines for Virtual Environment Management" on page 26.
- To maintain secure communication, you need the SSL certificates from your instances of vShield Manager. See "Obtain the SSL Certificate Thumbprint" on page 29.

Procedure

1. "Add vShield Manager Instances" on page 47

   Add the instances of vShield Manager to VCM so that you can license and collect vShield Manager data using the Managing Agent.

2. "Configure the vShield Manager Settings" on page 48

   Configure the Managing Agent, communication, and vShield Manager access options so that VCM can collect group and group member data from your instances of vShield Manager.

   "Collect vShield Manager Data" on page 49
3. Collect the data from the instances of vShield Manager. The data is displayed by detailed data type and appears in the VCM Console.

The collected vShield Manager data appears in the Console in the Virtual Environments node. See "vShield Manager Collection Results" on page 50.

Add vShield Manager Instances

Add the instances of vShield Manager to VCM so that you can license and collect vShield Manager data using the Managing Agent.

Most vShield Manager instances are discovered, added, and licensed. Use this procedure if they are not added to VCM.

Prerequisites

- Ensure that the vCenter Server that each instance of vShield Manager is managing is added to VCM. See "Add vCenter Server Instances" on page 30.
- Know the names and domain information for the instances of vShield Manager in your environment.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Available Machines**.
3. Click **Add Machines**.
4. On the Add Machines page, select **Basic: Name, Domain, Type**, **Automatically license machines**, and click **Next**.
5. On the Manually Add Machines - Basic page, configure these options to identify the instances of vShield Manager.

Option	Description
Machine	Name of the instance of vShield Manager.
Domain	Domain to which the instance of vShield Manager belongs.
Type	Domain type.
Machine Type	Select vShield.

6. Click **Add**.

   The machine information is added to the list.

7. (Optional) Add other instances of vShield Manager as needed.
8. When all your instances of vShield Manager are added to the list, click **Next**.
9. On the Information page, review the summary and click **Finish**.

What to do next

Configure the vShield Manager settings. See "Configure the vShield Manager Settings" on page 48.

Configure the vShield Manager Settings

Configure the Managing Agent, communication, and vShield Manager access options so that VCM can collect group and group member data from your instances of vShield Manager.

Prerequisites

- Collect Machines data from the Windows machine that you designated as your Managing Agent. See "Collect Machines Data From the Managing Agent Machines" on page 26.
- If you are using SSL Certificates to maintain secure communication, you must provide the certificate thumbprint from the target system when configuring the settings. See "Obtain the SSL Certificate Thumbprint" on page 29.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed Virtual Environments**.
3. Select the instances of vShield Manager and click **Configure Settings**.
4. On the Virtual Environment page, verify that the vShield Manager instances appear in the lower pane and click **Next**.

5. On the Managing Agent and Communication Settings page, configure the settings that are applied to all selected vShield Manager instances and click **Next**.

Option	Description
Managing Agent	Select the Windows machine to manage communication between the Collector and the vShield Manager instances. This Windows machine must have the 5.5 Agent or later installed. You can use the Collector as your managing agent.
Port	Type the port used by the API on the vShield Manager instances. The default value is 443.
User ID	Type a vShield Manager instance user name. The user must have a vShield Manager administrative role or an unrestricted read only role.
Password	Type the password for the vShield Manager instance user ID.
Confirm Password	Type the password again.
Ignore untrusted SSL Certificate	Select one of the following certificate options. ■ Yes: Ignores the requirement for a valid signed certificate. ■ No: Requires a valid signed certificate.
Select vCenter for vShield	Select the vCenter Server instance managed by this vShield Manager instance.

6. If you selected No on the Managing Agent and Communication Settings page, you must type or paste the thumbprint string in the text box and click **Next**.
7. On the Important page, click **Finish**.

What to do next

Collect vCloud Director data. See "Collect vShield Manager Data" on page 49.

Collect vShield Manager Data

Collect the data from the instances of vShield Manager. The data is displayed by detailed data type and appears in the VCM Console.

Prerequisites

Configure the vShield Manager settings. See "Configure the vShield Manager Settings" on page 48.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed Virtual Environments**.
3. Select the vShield Manager instances and click **Collect** on the VCM toolbar.
4. On the Collection Type page, select **Machine Data** and click **OK**.
5. On the Machines page, verify that the Selected list includes all the vShield Manager instances from which you are collecting and click **Next**.
6. On the Data Types page, select the Virtualization that you want to collect from the vShield Manager instances and click **Next**.
7. On the Important page, resolve any conflicts and click **Finish**.

What to do next

Review the collected virtualization data. Click **Console** and select **Virtual Environments > vCloud Director**.

Discover the vApp virtual machines created by the vCloud Director and make them available in VCM. See "Discover vCloud Director vApp Virtual Machines" on page 43.

vShield Manager Collection Results

The collected vShield Manager data appears in the Console and is available to generate reports.

The displayed data is only as current as the last time you collected data from your vShield Manager instances.

Option	Description
Console	Displays collected vShield Manager instance data. Click **Console** and select**Virtual Environments > vCloud Director**.
Reports	Create and run configured vShield Manager reports.
Administration	Displays managed vShield Manager instances from which you are collecting data. Click **Administration** and select **Machines Manager > Licensed Machines > Licensed Virtual Environments** to view licensed vShield Manager instances.
Administration > Machine Groups	Dynamic machine groups based on vShield App instances security group membership and are used to limit the displayed data.

Configure ESX Service Console OS Collections

The ESX Service Console OS Linux data type data and the ESX logs are collected directly from the ESX operating systems, not from vCenter Server. Configure the ESX servers so that you can collect the Linux data type and ESX log data from the ESX service console operating system.

To collect the data, VCM uses an Agent Proxy rather than a VCM Agent installed directly on the ESX and ESXi machines. To support the Agent Proxy, you must copy required files and certificates on the ESX and ESXi servers to manage the data collection from those machines.

Perform the required tasks first for ESX servers, and then for ESXi servers.

1. "Configure the Collector as an Agent Proxy" on page 51

   The Agent Proxy machine is a Windows machine configured to communicate with ESX and ESXi servers and to remotely collect data from those servers. The Collector automatically meets the Agent Proxy requirements. You license the Collector and then collect the Machines data type.

2. "Configure Virtual Machine Hosts" on page 52

   License virtual machine hosts to generate a file containing machine names and settings. You use the generated file to configure the ESX machines for management in VCM.

3. "Copy Files to the ESX/ESXi Servers" on page 54

   To import target machine information and copy the required files from VCM, you use the UNIX/ESX/vSphere Deployment Utility on your Agent Proxy machines.

4. "Collect ESX Logs Data" on page 55

   An initial collection of Virtual Environments data identifies your virtual machine hosts and their guest machines.

You have several options for reviewing and using ESX Logs data in VCM. The data used is only as current as the last collection, and the amount of time it takes for the data to display is based on the volume or complexity of the data requested. See "Virtualization Collection Results" on page 56.

Configure the Collector as an Agent Proxy

The Agent Proxy machine is a Windows machine configured to communicate with ESX and ESXi servers and to remotely collect data from those servers. The Collector automatically meets the Agent Proxy requirements. You license the Collector and then collect the Machines data type.

NOTE If you manage more than fifty host machines, you must use a separate Windows machine as your Agent Proxy. Moving the Agent Proxy activity to the separate machine optimizes performance. See "Configuring Standalone Agent Proxy Machines" in the online Help.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed Windows Machines**.
3. Determine whether the Collector machine name appears in the data grid.

   If it is listed in the data grid, the machine is licensed. If it is not listed, continue with the licensing process.

4. License the Collector.
   a. Select **Machines Manager > Available Machines**.
   b. Select the Collector in the data grid and click **License**
   c. On the Machines page of the Available Machines License wizard, verify that the Collector machine name appears in the Selected list and click **Next**.
   d. Review the Product License Details page and click **Next**.
   e. Review the Important page and click **Finish**.
   f. Select **Administration > Machines Manager > Licensed Machines > Licensed Windows Machines** to verify that the Collector is now licensed.
   g. Click **Refresh** on the Console toolbar to update the data.
5. Run a collection for machines data to identify the Collector as an available Windows machine.
   a. Select **Machines Manager > Licensed Windows Machines**, select the Collector in the data grid, and click **Collect** on the Console toolbar.
   b. On the Collection Type page, click **Machine Data** and click **OK**.
   c. On the Machines page, verify that the Collector machine name appears in the Selected list.
   d. Click **Select Data Types to collect from these machines** and click **Next**.
   e. On the Data Types page, expand the Windows tree and select **Machines**.
   f. Select **Use default filters** and click **Next**.
   g. Review the Important page and click **Finish**.

      The collection job starts. You can use the Job Manager to determine when the collection is finished.

What to do next

- When the collection is completed, verify that the Collector machine Agent Proxy State equals Current Agent. Click **Administration** and select **Machines Manager > Agent Proxies** and review the data grid.
- License and configure the target virtual machine hosts. See "Configure Virtual Machine Hosts" on page 52.

Configure Virtual Machine Hosts

License virtual machine hosts to generate a file containing machine names and settings. You use the generated file to configure the ESX machines for management in VCM.

All Virtualization data types are collected through Web Services communication except for the VM Logs, which are collected through SSH and only from ESX machines.

Prerequisites

Verify that at least one Agent Proxy machine is configured. See "Configure the Collector as an Agent Proxy" on page 51.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed ESX/ESXi Hosts**.
3. Select the ESX host and click **Configure Settings**.
4. Add the machines to be configured to the lower grid and click **Next**.

   The selected machines will use the same Agent Proxy and the same SSH and Web Services settings.
5. Configure the settings on the Agent Proxy and Communication Setting page.

Option	Description
Agent Proxy	The configured Agent Proxy used to manage the selected virtual machine host machines. This option is required when you are licensing host machines, but it is optional if you are modifying the settings.
SSH Settings	Select the check box to configure the settings for your ESX machines. Configure these settings so that you can collect ESX Logs data from the managed host machines. ■ **Port:** Used by VMware Web Services SDK for the ESX server on which SSH listening. The Agent Proxy communicates with the ESX server using this port. The default port (22) is set to the default value for SSH on ESX. ■ **User ID:** Used by the Agent Proxy to communicate with the ESX server through SSH. This account must have certain permissions, for example, `sudoers`, defined in the installation process. Authentication for this account uses public key cryptography that was setup during the installation process.
Web Services Settings	(Optional) Select the check box to configure the settings for your ESX and ESXi machines. Configure the settings to collect virtual environment data from a host machine. ■ **Port:** The port on the ESX server used by the Agent Proxy to communicate with the VMware web services interface. ■ **User ID:** The account that has access to the VMware Web services interface. If you are using ESX, this account must have Administrator access to Web services on the ESX server. This user ID may be different from the user ID for SSH communication, depending on whether you created different accounts during the ESX installation process. ■ **Password:** The password for the Web services User ID specified above. This password is encrypted in the VCM database. ■ **Confirm Password:** Retype the password. ■ **Ignore untrusted SSL Certificate:** Connection allowed even when certificates are not verified as trusted.

6. On the Important page, record the `.xml` file name.

   The file is saved to the location configured for `CMFiles$\VMHosts_Config`. The default location is `\Program Files (x86)\VMware\VCM\WebConsole\L1033\Files\VMHosts_Config`.
7. Click **Finish**.

What to do next

Copy the copy SSH public key file, the `csiprep.py` file, and the `csiprep.config` file to the target ESX machines. See "Copy Files to the ESX/ESXi Servers" on page 54.

Copy Files to the ESX/ESXi Servers

To import target machine information and copy the required files from VCM, you use the UNIX/ESX/vSphere Deployment Utility on your Agent Proxy machines.

For ESX machines, you import target machine information from VCM and copy the SSH public key file, the `csiprep.py` file, and the `csiprep.config` file to the target ESX machines.

For ESXi machines, you import machine information and copy the necessary Web Services settings to the target machines.

Prerequisites

- License the ESX and ESXi machines. See "Configure Virtual Machine Hosts" on page 52.
- Locate the UNIX/ESX/vSphere Deployment Utility file in `C:\Program Files (x86)\VMware\VCM\Tools\DeployUtility-<version number>`. Consult the Deployment Utility online help when using the tool.

Procedure

1. Copy the UNIX/ESX/vSphere Deployment Utility file to the Agent Proxy machine, either a standalone Windows machine or the Collector, and unzip the file.
2. Double-click `DeployUtil.exe` to start the Deployment Utility.
3. Click the **ESX/vSphere Configuration** tab.
4. Click **File > Open**.
5. Browse to the location of the virtual machine hosts configuration file generated when you licensed and configured the virtual machine hosts.

   The default location on the Collector is `\Program Files (x86)\VMware\VCM\WebConsole\L1033\Files\VMHosts_Config`.
6. Select the `.xml` file and click **Open**.

   The machine information in the `.xml` file is imported into the **ESX Server Settings** table on the **ESX/vSphere Configuration** tab with the settings that you defined in VCM.
7. Select a configuration option.

Option	Description
Configure ESX 3.x Servers	Configures the SSH certificate, the `csiprep.py` file, the `csiprep.config` file, and passes the SSH and Web Services user information to the target ESX machines.
Configure ESXi Servers	Passes the Web Services to the target ESX machines

8. (Optional) Configure the default server location.

   The following settings are automatically configured to the default server locations. If you need to change the paths, click the ellipsis button.

   - SSH Public Key file (ESX 3.x only)
   - Log Files Location
   - `csiprep.py` File (ESX 3.x only)
   - `csiprep.config` File (ESX 3.x only)

9. (Optional) Configure the VCM user name and password.

   To modify the settings in VCM, use the following options or manually change the values in the ESX Server Settings table. For more information about the settings, see the Deployment Utility online Help.

   - Use the same user name for both SSH and Web Services collections (ESX 3.x only).
   - Use the same password for all WebServices users.
   - Apply the same user names and passwords to all ESX servers.

10. Click **Configure**.

    All the machines where the **Configure** check box is selected now have the same version of the files copied to the location specified in the Remote Path field in the table. If no path is specified, the files are copied to the `/tmp` directory.

What to do next

Collect data from the target virtual machine hosts. See "Collect ESX Logs Data" on page 55.

Collect ESX Logs Data

An initial collection of Virtual Environments data identifies your virtual machine hosts and their guest machines.

Procedure

1. On the Portal toolbar, click **Collect**.
2. Select your ESX Servers.

   To avoid configuration conflicts, do not select both for one action. The selected machines appear in the Selected list.

3. Click **Select Data Types to collect from these machines** and click **Next**.
4. Expand the UNIX node and select the **Machines - General** data type.
5. Expand the Virtualization node and select the **ESX Logs** data types.
6. Click **Use default filters** and click **Next**.
7. Click **Finish**.

Monitor the collection job in Job Manager. When the collection is completed, the data appears is available for reports and compliance assessments.

What to do next

Review the collected data in the Console, run reports, configure alerts, and use the machine groups. See "Virtualization Collection Results" on page 56.

Virtualization Collection Results

You have several options for reviewing and using ESX Logs data in VCM. The data used is only as current as the last collection, and the amount of time it takes for the data to display is based on the volume or complexity of the data requested.

Option	Description
Console	View ESX logs. Click **Console** and select **Virtual Environments > ESX Logs**.

Configure the vSphere Client VCM Plug-In

The vSphere Client VCM Plug-In provides contextual access to VCM change, compliance, and management functions. It also provides direct access to collected vCenter Server, virtual machine host, and virtual machine guest data.

When using the vSphere Client VCM Plug-In, the virtual machine host name in vCenter must match the virtual machine host name in VCM.

CAUTION Anyone accessing VCM and the vSphere Client must have a unique login. Do not share vSphere Client logins between VCM users. Do not share vSphere Client logins between VCM users and non-VCM users.

Procedure

1. "Register the vSphere Client VCM Plug-In" on page 56

   The registration process configures the URL in the VMware vSphere Client to the VCM Collector and makes the **VCM Summary** and **VCM Actions** tabs available in the vSphere Client.

2. "Configuring the vSphere Client VCM Plug-In Integration Settings" on page 57

   Configure integration settings in VCM for your vSphere Client VCM Plug-In users. The settings enable users to view the VCM reports.

3. "Manage Machines from the vSphere Client" on page 58

   vSphere Client-managed machines are available in the vSphere Client VCM Plug-In when they licensed and have the VCM Agent installed. The available actions include collecting new data and running compliance, patching, and reports for the selected machines.

Register the vSphere Client VCM Plug-In

The registration process configures the URL in the VMware vSphere Client to the VCM Collector and makes the **VCM Summary** and **VCM Actions** tabs available in the vSphere Client.

The plug-in is installed with VCM. To unregister a previous version of the plug-in, see the online Help.

IMPORTANT The account that you use to register the vSphere Client VCM Plug-In should be a local administrator on the vSphere instance. The account must connect to a machine that has a valid SSL certificate or must register an invalid certificate (for example, a development certificate) when that user logs into the vSphere Client.

Prerequisites

- Verify that you are using VMware vCenter 4 Server.
- Verify that the VMware vSphere Client is installed.
- Verify that the VMware Tools is installed on the virtual machines.

Procedure

1. On the VCM Collector, browse to `[path]\VMware\VCM\Tools\vSphere Client VCM Plugin\bin` and double-click `VCVPInstaller.exe`.
2. In the VCVP Plug-in Registration dialog box, configure the following options.

Option	Description
Register	Select the option to register the URL for the plug-in. Select Unregister only if you are discontinuing the use of the plug-in on the target vSphere Client.
Server URL	Type the http or https path, where <server> is your vSphere Client server.
Administrator User Name	Type the name of a user with Administrator privileges in the vSphere Client.
Administrator Password	Type the associated password.
URL to vSphereClientVCMPlugin.xml	Type the http path, where <VCMserver> is the name or IP address for the VCM Collector. The xml file is located in `\VMware\VCM\WebConsole\L1033\VCVPAnon\Xml\vSphereClientVCMPlugin.xml`

3. Click **OK**.
4. Start VCM.
5. On the login screen, select the role that you are using to log into the vSphere Client VCM Plug-In.
6. Select the **Automatically log in using this role** check box.
7. Start the vSphere Client.
8. Select a Guest machine.

What to do next

- Confirm that you can access the **VCM Summary** and **VCM Actions** tabs.
- Configure the vSphere Client VCM Plug-In integration settings in VCM. See "Configuring the vSphere Client VCM Plug-In Integration Settings" on page 57.

Configuring the vSphere Client VCM Plug-In Integration Settings

Configure integration settings in VCM for your vSphere Client VCM Plug-In users. The settings enable users to view the VCM reports.

Prerequisites

Verify that the vSphere Client VCM Plug-In is registered. See "Register the vSphere Client VCM Plug-In" on page 56.

Procedure

1. Select **Administration > Settings > Integrated Products > VMware > vSphere Client VCM Plug-In**.
2. Select the setting that you want to configure and click **Edit Settings**.
3. On the Settings Wizard page for each setting, configure the options.

Option	Description
Machine group against which the external reports will be run	Type the name of the machine group. The default value is All Machines.
Role to use for external report access	Type the name of the user role to be used to access the reports. The default value is Read-Only. Users other than Admin must have the role selected here in order to see reports in the vSphere Client.
User name to use for assessments	Type the name of the user who will run assessments to obtain data for generating reports.

4. Click **Next**.
5. Verify your settings and click **Finish**.

What to do next

You manage machines by running compliance, patching, and reports. See "Manage Machines from the vSphere Client" on page 58.

Manage Machines from the vSphere Client

vSphere Client-managed machines are available in the vSphere Client VCM Plug-In when they licensed and have the VCM Agent installed. The available actions include collecting new data and running compliance, patching, and reports for the selected machines.

Prerequisites

- Verify that the integration settings are configured. See "Configuring the vSphere Client VCM Plug-In Integration Settings" on page 57.
- Configure your virtual machines for VCM management. See "Configure Windows Machines" on page 87 and "Configure Collections from Linux, UNIX, and Mac OS X Machines" on page 120.

Procedure

1. Start the vSphere Client.
2. Click the **VCM Actions** tab.

What to do next

Click help on the **VCM Actions** tab for more information about the actions.

Running Compliance for the VMware Cloud Infrastructure

4

Compliance templates evaluate the virtual environment object data to determine if the objects meet the criteria in the rules. If the property values on an object do not meet the criteria, and if there is no exception defined, then the object is flagged as noncompliant. When an object is non compliant, the template results provide the details of the settings or configurations that do not match the rules. You can use this information to resolve the issue.

Compliance templates include the following components:

- **Rule Groups:** The rule groups comprise rules and filters.
- **Rules:** The rules define the optimal configuration standard.
- **Filters:** The filters limit the objects on which the template runs to only the objects that meet the filter criteria. If filters are not defined, the rules are run against all objects in the virtual objects group.
- **Exceptions:** The exceptions are optional temporary or permanent exceptions to the template results. The defined exception indicates that a specific result is compliant or noncompliant even though it does not match the requirements of the rules.

After you configure your compliance templates, you can optimize how VCM monitors the compliance of objects in your environment using alerts and scheduling regular compliance template runs on your collected virtual environment data.

This chapter includes the following topics:

Create and Run Virtual Environment Compliance Templates 59
Create Virtual Environment Compliance Rule Groups 60
Create and Test Virtual Environment Compliance Rules 61
Create and Test Virtual Environment Compliance Filters 62
Preview Virtual Environment Compliance Rule Groups 62
Create Virtual Environment Compliance Templates 63
Run Virtual Environment Compliance Templates 64
Create Virtual Environment Compliance Exceptions 65
Resolve Noncompliant Virtual Environments Template Results 66
Configure Alerts and Schedule Virtual Environment Compliance Runs 68

Create and Run Virtual Environment Compliance Templates

Create compliance templates that evaluate your virtual environment object data to determine if the objects meet the criteria in the rules that define objects as compliant or noncompliant.

The example used in this procedure is whether VMware Tools is running on guest virtual machines on all vCenter Server instances, but excluding vCenter_Dev.

Prerequisites

Collect virtual environments data. See "Configure Virtual Environments Collections" on page 25.

Procedure

1. "Create Virtual Environment Compliance Rule Groups" on page 60

   Rule groups contain compliance rules and filters. You must create rule groups that you then assign to compliance templates.

2. "Create and Test Virtual Environment Compliance Rules" on page 61

   You create rules that define the ideal values that objects should have to be considered compliant.

3. "Create and Test Virtual Environment Compliance Filters" on page 62

   You can create filters that limit the objects on which the templates run to only the objects that meet the filter criteria.

4. "Preview Virtual Environment Compliance Rule Groups" on page 62

   You use the rules preview action, with the filters turned off and then turned on, to determine if a rule group is returning the expected results.

5. "Create Virtual Environment Compliance Templates" on page 63

   You can create compliance templates that include one or more rule groups that assess your selected object group to determine which objects are compliant and noncompliant.

6. "Run Virtual Environment Compliance Templates" on page 64

   You run templates against your collected data to determine which objects are compliant or noncompliant.

7. "Resolve Noncompliant Virtual Environments Template Results" on page 66

   The results for the compliance templates indicate whether the virtual or physical machine are compliant or noncompliant. If the machine is noncompliant, you can enforce noncompliant results manually or using VCM, or you can add an exception for expected noncompliant results.

Create Virtual Environment Compliance Rule Groups

Rule groups contain compliance rules and filters. You must create rule groups that you then assign to compliance templates.

Templates can include one or more rule groups. Rule groups comprise rules and filters.

The example used in this procedure is whether VMware Tools is running on guest virtual machines on all vCenter Server instances, but excluding vCenter_Dev.

Procedure

1. Click **Compliance**.
2. Select **Virtual Environment Compliance > Rule Groups**.
3. Click **Add**.
4. Type the Rule Group Name and Description in the text boxes and click **OK**.

   For example, Guest Tools Running and a description.

What to do next

Add a rule to the rule group. See "Create and Test Virtual Environment Compliance Rules" on page 61.

Create and Test Virtual Environment Compliance Rules

You create rules that define the ideal values that objects should have to be considered compliant.

The data types correspond to the collected virtual environments data that is displayed in the Console. To identify the values you are configuring for compliance, review the data grids so that you can locate the correct data type in the rule wizard.

The example used in this procedure is whether VMware Tools is running on guest virtual machines on all vCenter Server instances, but excluding vCenter_Dev.

Prerequisites

Create a rule group. See "Create Virtual Environment Compliance Rule Groups" on page 60.

Procedure

1. Click **Compliance**.
2. Select **Virtual Environment Compliance > Rule Groups > rule group name > Rules**.

   Guest Tools Running is the rule group in this example.
3. Click **Add**.
4. Type the Name and Description in the text boxes and click **Next**.

   For example, Tools Running.
5. Expand **Virtualization**, select **vCenter - Guests - Summary**, and click **Next**.

   The collected guest summary data includes whether the VMware Tools is installed and running on the guest virtual machines.
6. Select **Basic** and click **Next**.
7. Click **Add** and configure the rules with the ideal values.
   - In the properties drop-down menu, select **Tools Running Status**.
   - Select = as the rule operator.
   - Click the ellipsis button and select **guestToolsRunning** and click **OK**.
   - Click **Next**.
8. Select the Severity of a failure in the drop-down menu and click **Next**.
9. Review the changes and click **Finish**.

   The rule is added to the data grid.
10. Select your new rule and click **Preview**.
11. Select **Do not apply machine filters to preview** and click **OK**.

    When you test a rule, test first without the filter to ensure that the rule returns the expected results.
12. Review the data in the Non-compliant results window to verify that your rule is behaving as expected.

What to do next

Add a filter to the rule group. See "Create and Test Virtual Environment Compliance Filters" on page 62.

Create and Test Virtual Environment Compliance Filters

You can create filters that limit the objects on which the templates run to only the objects that meet the filter criteria.If filters are not defined, the rules are run against all objects in the selected virtual objects group.

The example used in this procedure is whether VMware Tools is running on guest virtual machines on all vCenter Server instances, but excluding vCenter_Dev.

Prerequisites

- Create a rule group. See "Create Virtual Environment Compliance Rule Groups" on page 60.
- Create a rule. See "Create and Test Virtual Environment Compliance Rules" on page 61.

Procedure

1. Click **Compliance**.
2. Select **Virtual Environment Compliance > Rule Groups > rule group name > Filters**.

   Guest Tools Running is the rule group in this example.
3. Click **Add**.
4. Type the Name and Description in the text boxes and click **Next**.

   For example, Not vCenter_Dev
5. Expand **Virtualization**, select **vCenter - Guest - Summary**, and click **Next**.

   The collected guest summary data includes vCenter names.
6. Select **Basic** and click **Next**.
7. Click **Add** and configure the filter with the values to limit assessed objects or to exclude objects from assessment.
   - In the properties drop-down menu, select **vCenter**.
   - Select <> as the filter operator.
   - Click the ellipsis and select **vCenter_Dev** and click **OK**.
   - Click **Next**.
8. Review the changes and click **Finish**.

   The filter is added to the data grid.
9. Select your new filter and click **Preview**.
10. Review the data in the Machines window to verify that your filter is behaving as expected.

What to do next

Test your rule and filter together. See "Preview Virtual Environment Compliance Rule Groups" on page 62.

Preview Virtual Environment Compliance Rule Groups

You use the rules preview action, with the filters turned off and then turned on, to determine if a rule group is returning the expected results.

The example used in this procedure is whether VMware Tools is running on guest virtual machines on all vCenter Server instances, but excluding vCenter_Dev.

Prerequisites

- Create a rule group. See "Create Virtual Environment Compliance Rule Groups" on page 60.
- Create a rule. See "Create and Test Virtual Environment Compliance Rules" on page 61.
- Create compliance filters. See "Create and Test Virtual Environment Compliance Filters" on page 62.

Procedure

1. Click **Compliance**.
2. Select **Virtual Environment Compliance > Rule Groups**.

   Guest Tools Running is the rule group in this example.
3. Select your new rule group and click **Preview**.
4. Select **Do not apply machine filters to preview** and click **OK**.

   When you test a rule, test first without the filter to ensure that the rule returns the expected results.
5. Review the data in the Non-compliant results window to verify that your rule is behaving as expected.
6. Close the window.
7. Select your new rule group and click **Preview**.
8. Select **Apply machine filters to preview** and click **OK**.
9. Review the data in the Non-compliant results window to verify that your rule is behaving as expected. If the results are incorrect, adjust your rules and filters until they work correctly when you preview them.

What to do next

- If you have more than one rule that you must run in a particular order, set the order. The Set Order option is located on the toolbar.
- Create a template. See "Create Virtual Environment Compliance Templates" on page 63.

Create Virtual Environment Compliance Templates

You can create compliance templates that include one or more rule groups that assess your selected object group to determine which objects are compliant and noncompliant.

The example used in this procedure is whether VMware Tools is running on guest virtual machines on all vCenter Server instances, but excluding vCenter_Dev.

Prerequisites

Create a rule group. See "Create and Test Virtual Environment Compliance Rules" on page 61.

Procedure

1. Click **Compliance**.
2. Select **Virtual Environment Compliance > Templates**.
3. Click **Add**.
4. Type the Name and Description in the text boxes and click **Next**.

   For example, Tools Running Not vCenter_Dev and a description.
5. Move the rule group, for this example, Guest Tools Running, to the list on the right and click **Next**.
6. Select **Return both compliant and non-compliant** and click **Next**.

   Returning complaint and noncompliant results will help you determine whether your template is returning the correct results.
7. Review your changes and click **Finish**.

What to do next

Run the template. See "Run Virtual Environment Compliance Templates" on page 64.

Run Virtual Environment Compliance Templates

You run templates against your collected data to determine which objects are compliant or noncompliant.

When a compliance template is run, the results appear in a report format and a data grid format.

The example used in this procedure is whether VMware Tools is running on guest virtual machines on all vCenter Server instances, but excluding vCenter_Dev.

Prerequisites

Create a template. See "Create Virtual Environment Compliance Templates" on page 63.

Procedure

1. Click **Compliance**.
2. Select **Virtual Environment Compliance > Templates**.
3. Select your template in the data grid and click **Run**.

   In this example, select Tools Running Not vCenter_Dev.
4. Click **OK**.
5. When the template run is finished, click **Close**.
6. Double-click the template name in the data grid.

   Unless you turned off the summary view, the Virtual Environments Compliance Results report appears. The report includes the number of objects that are compliant and the number that are noncompliant.
7. To view the results in the data grid, click **View data grid**.

What to do next

- If you find results that you want to temporarily make compliant or noncompliant, create an exception. See "Create Virtual Environment Compliance Exceptions" on page 67.
- Evaluate the results and resolve any issues on the noncompliant objects.

Create Virtual Environment Compliance Exceptions

To temporarily or permanently override the specific template results, use exceptions rather than explicitly resolve noncompliant results.

The exceptions are defined against the template results and indicate that a specific result is compliant or noncompliant even though it does not match the requirements of the rules.

You can add exceptions only to existing templates.

The example used in this procedure is whether VMware Tools is running on guest virtual machines on all vCenter Server instances, but excluding vCenter_Dev.

To create an exception in this example, a virtual machine, RHEL_60_ProdDev, is approved to be excluded from the noncompliant results because you never require VMware Tools to be running on this machine.

Prerequisites

Create a template. See "Create Virtual Environment Compliance Templates" on page 63.

Procedure

1. Click **Compliance**.
2. Select **Virtual Environment Compliance > Templates > template name**.
3. In the data grid, select the noncompliant result on which you are basing the exception and click **Add Exception**.

   In this example, the noncompliant result is the RHEL_60_ProdDev guest machine.
4. Type the Name, Short Description, Description, and Sponsor in the text boxes and click **Next**.
5. Select the template to which you are applying the exception in the drop-down menu and click **Next**.

   For this example, select Tools Running Not vCenter_Dev.
6. Select the object group to which you are applying the exception and click **Next**.

   For this example, select All Virtual Objects.
7. Select the override options and the expiration date.
   a. Select **Override non-compliant results to compliant**.
   b. Select **No Expiration**.
   c. Click **Next**.

8. To define the exception values, modify, delete, or add to the properties, operators, and values for the selected results.

   In this example, you are specifying the RHEL_60_ProdDev as the exception.

   a. Click **Add**.

   b. In the properties drop-down menu, select **Object**.

   c. Select = as the rule operator.

   d. Click the ellipsis button and select **RHEL_60_ProdDev** in the property values dialog box and click **OK**.

9. Click **Finish**.

What to do next

- Run the template. See "Run Virtual Environment Compliance Templates" on page 64.
- Create alerts and schedule regular runs of your compliance templates. See "Configure Alerts and Schedule Virtual Environment Compliance Runs" on page 68

Resolve Noncompliant Virtual Environments Template Results

The results for the compliance templates indicate whether the virtual or physical machine are compliant or noncompliant. If the machine is noncompliant, you can enforce noncompliant results manually or using VCM, or you can add an exception for expected noncompliant results.

These procedures provide a variety of examples that apply to virtual environments compliance.

Procedure

1. "Enforce Compliance Template Results by Using VCM Actions" on page 190

   You can resolve noncompliant results using VCM actions on the data grids to change settings when the action is not available for enforceable compliance.

2. "Manually Enforce Compliance Template Results" on page 191

   You can resolve noncompliant results by directly accessing the virtual or physical machine, or by accessing the object in vCenter Server, to change the noncompliant configuration setting.

3. "Create Virtual Environment Compliance Exceptions" on page 67

   To temporarily or permanently override the specific template results, use exceptions rather than explicitly resolve noncompliant results.

Enforce Compliance Template Results by Using VCM Actions

You can resolve noncompliant results using VCM actions on the data grids to change settings when the action is not available for enforceable compliance.

For this example, a template includes a rule that requires virtual machines to be powered on. If a virtual machine is powered off, the object is noncompliant. The compliance remediation action is to power it on.

Procedure

1. Click **Compliance**.
2. Select **Virtual Environments Compliance > Templates > {template name}**.
3. In the Status column, identify the rule results that are noncompliant.
4. Identify the affected physical or virtual machines or virtual objects, and determine the expected value of the property.

   For example, click and drag the Status column heading and the Rule column heading to the filter. Expand the noncompliant results and the rule related to the power state. The noncompliant object appears in the object column.
5. To resolve the noncompliant results, click **Console** and select **Virtual Environments**, the **Windows tab**, or the **UNIX tab**, and browse to the data grid where the action is available.

   For example, click **Console** and select **Virtual Environments > vCenter > Guests > Summary**.
6. Select the machines or objects that you identified as noncompliant and click the applicable action button on the data grid.

   For example, select the virtual machines that are powered off that should be powered on to be compliant and click **Power VM On**.
7. Follow the prompts to configure the options, select **Run action now**, and click **Finish**.

What to do next

Collect the appropriate data from the physical or virtual machines or objects and run compliance against the collected data. The objects should now be compliant.

Manually Enforce Compliance Template Results

You can resolve noncompliant results by directly accessing the virtual or physical machine, or by accessing the object in vCenter Server, to change the noncompliant configuration setting.

Procedure

- Using your allowed methods, change the noncompliant setting value on the machine or object to the required compliant value.

What to do next

Collect the appropriate data from the virtual or physical machines or objects and run compliance against the collected data. The objects should now be compliant.

Create Virtual Environment Compliance Exceptions

To temporarily or permanently override the specific template results, use exceptions rather than explicitly resolve noncompliant results.

The exceptions are defined against the template results and indicate that a specific result is compliant or noncompliant even though it does not match the requirements of the rules.

You can add exceptions only to existing templates.

The example used in this procedure is whether VMware Tools is running on guest virtual machines on all vCenter Server instances, but excluding vCenter_Dev.

To create an exception in this example, a virtual machine, RHEL_60_ProdDev, is approved to be excluded from the noncompliant results because you never require VMware Tools to be running on this machine.

Prerequisites

Create a template. See "Create Virtual Environment Compliance Templates" on page 63.

Procedure

1. Click **Compliance**.
2. Select **Virtual Environment Compliance > Templates > template name**.
3. In the data grid, select the noncompliant result on which you are basing the exception and click **Add Exception**.

   In this example, the noncompliant result is the RHEL_60_ProdDev guest machine.
4. Type the Name, Short Description, Description, and Sponsor in the text boxes and click **Next**.
5. Select the template to which you are applying the exception in the drop-down menu and click **Next**.

   For this example, select Tools Running Not vCenter_Dev.
6. Select the object group to which you are applying the exception and click **Next**.

   For this example, select All Virtual Objects.
7. Select the override options and the expiration date.
   a. Select **Override non-compliant results to compliant**.
   b. Select **No Expiration**.
   c. Click **Next**.
8. To define the exception values, modify, delete, or add to the properties, operators, and values for the selected results.

   In this example, you are specifying the RHEL_60_ProdDev as the exception.
   a. Click **Add**.
   b. In the properties drop-down menu, select **Object**.
   c. Select = as the rule operator.
   d. Click the ellipsis button and select **RHEL_60_ProdDev** in the property values dialog box and click **OK**.
9. Click **Finish**.

What to do next

- Run the template. See "Run Virtual Environment Compliance Templates" on page 64.
- Create alerts and schedule regular runs of your compliance templates. See "Configure Alerts and Schedule Virtual Environment Compliance Runs" on page 68

Configure Alerts and Schedule Virtual Environment Compliance Runs

To optimize how VCM monitors the compliance of objects in your environment, configure alerts and schedule regular compliance template runs on your collected virtual environment data.

Prerequisites

Create at least on virtual environments compliance template. See "Create and Run Virtual Environment Compliance Templates" on page 59.

Procedure

1. "Create Virtual Environment Compliance Alert Rules" on page 69

   Alert rules are the conditions you define that determine when an alert is generated. Virtual environment alert rules are based on virtual environment compliance templates.

2. "Create Virtual Environments Compliance Alert Configurations" on page 69

   Virtual environment compliance alert configurations are created for virtual object groups to generate alerts when a virtual environment compliance template returns noncompliant results during scheduled runs of the template.

3. "Schedule Virtual Environments Compliance Template Runs" on page 70

   You can schedule a regular run of your virtual environments compliance templates to ensure that the collected data is regularly assessed for adherence to the defined compliance rules.

Create Virtual Environment Compliance Alert Rules

Alert rules are the conditions you define that determine when an alert is generated. Virtual environment alert rules are based on virtual environment compliance templates.

Prerequisites

Verify that you have virtual environment compliance templates. See "Create and Run Virtual Environment Compliance Templates" on page 59.

Procedure

1. Click **Administration**.
2. Select **Alerts > Rules**.
3. Click **Add**.
4. Type the alert name and description in the text boxes and click **Next**.
5. Select **VE Compliance Results Data** and click **Next**.
6. Select a compliance template and click **Next**.
7. Review the configured actions and click **Finish**.

What to do next

Create a virtual environments configuration that includes this rule. See "Create Virtual Environments Compliance Alert Configurations" on page 69.

Create Virtual Environments Compliance Alert Configurations

Virtual environment compliance alert configurations are created for virtual object groups to generate alerts when a virtual environment compliance template returns noncompliant results during scheduled runs of the template.

You must have at least one unused rule to add to the alert configuration parameters.

Prerequisites

- Verify that you have virtual environment alert rules. See "Create Virtual Environment Compliance Alert Rules" on page 69.
- Review the automated response options, which you configure in this procedure, in the online Help.

Procedure

1. Click **Administration**.
2. Select **Alerts > Virtual Environments Configurations**.
3. In the middle pane, select the virtual objects group for which you want to generate an alert if one or more rules in the template fail.
4. Click **Add**.
5. Select a virtual environments compliance results alert rule and click **Next**.
6. Select the alert severity and click **Next**.

   You can select Critical, Important, Moderate, or Low.
7. Select and configure one or more automated responses that are performed when an alert is generated and click **Next**.

   Depending on the automated responses you selected, the pages will vary. See the online Help for configuration details.
8. Review the alert configuration and click **Finish**.

What to do next

Schedule a job to run your the virtual environments compliance templates on a timetable of your choosing. See "Schedule Virtual Environments Compliance Template Runs" on page 70.

Schedule Virtual Environments Compliance Template Runs

You can schedule a regular run of your virtual environments compliance templates to ensure that the collected data is regularly assessed for adherence to the defined compliance rules.

Compliance templates are run against collected data, so you should also schedule collections for the data types and virtual objects that you are assessing.

Prerequisites

- Schedule a regular collection of the virtual environments data types for the virtual object groups against which you are running the virtual environments compliance templates.
- Create Virtual Environments Compliance Template. See "Create and Run Virtual Environment Compliance Templates" on page 59.
- Create Virtual Environments Compliance Alerts. See "Create Virtual Environment Compliance Alert Rules" on page 69.

Procedure

1. Click **Administration**.
2. Select **Job Manager > Scheduled**.
3. Click **Add**.
4. Select **Compliance** and click **Next**.
5. Type a name and description in the text boxes and click **Next**.
6. Select the virtual environment template and click **Next**.
7. Select the virtual objects against which to run the template assessment and click **Next**.
8. Configure frequency, time of day, and duration for the job and click **Finish**.
9. To test whether the job is producing the expected results, click **Run Now** on the data grid toolbar.

The job runs at the scheduled time.

What to do next

If you a configured virtual environments compliance alert for this template and non-compliant rules were found, you can review any alerts in the Alerts node in the Console.

Configuring vCenter Operations Manager Integration 5

Integration of VCM with vCenter Operations Manager reports VCM configuration change events and standard compliance results in vCenter Operations Manager.

This chapter includes the following topics:

Configure vCenter Operations Manager Change Events 73

Standards Compliance for vCenter Operations Manager 74

VCM Registration in vCenter Operations Manager for Integration

Integration between VCM and vCenter Operations Manager uses an adapter to manage the connection.

When you register the VCM adapter in the vCenter Operations Manager Administration portal, ensure that the user account used for the integration meets the following criteria:

- The account is used only by the adapter login. The account must not be one used as an interactive user login. The adapter account frequently logs in and out of VCM. If you use it as an interactive account, you will need to regularly refresh the connection, which affects your VCM experience.
- The account has permission in VCM to access the virtual object groups and machine groups that correspond to the objects managed by your vCenter Operations Manager instance.

For more information about registering the VCM adapter, see the vCenter Operations Manager Administration portal online Help.

Configure vCenter Operations Manager Change Events

Configure the data types to report to vCenter Operations Manager as change events and the threshold reporting level used to roll up the configuration changes. VCM records configuration changes in the change log regardless of whether you report the data in vCenter Operations Manager. From vCenter Operations Manager, you can navigate to VCM to view the details.

You can report on UNIX and Windows configuration change data and VCM initiated reboot changes. VCM reports change data to vCenter Operations Manager. vCenter Operations Manager polls VCM for configuration changes every five minutes.

For example, you can configure VCM to report a UNIX data type to vCenter Operations Manager and set the threshold reporting level to roll up a defined number of configuration changes into a single reporting icon to report the changes in the vCenter Operations Manager console.

Prerequisites

Ensure that the VCM adapter is registered with the correct user account in vCenter Operations Manager. See "VCM Registration in vCenter Operations Manager for Integration" on page 73.

Procedure

1. In VCM, click **Administration**.
2. Select **Settings > Integrated Products > VMware > vCenter Operations Manager > Change Events**.
3. Configure VCM to report a UNIX data type, such as UNIX Patch Assessment, to vCenter Operations Manager.
   a. Select **UNIX Patch Assessment - Report to vCenter Operations Manager**, and click **Edit Setting**.
   b. Click **Yes** to report the data.
   c. Click **Next** and click **Finish**.
4. Set the threshold reporting level to roll up the configuration changes in the vCenter Operations Manager console.
   a. Select **UNIX Patch Assessment - Rollup Threshold**, and click **Edit Setting**.
   b. Type the number of configuration changes for the collection to roll up to a single reporting icon to report in vCenter Operations Manager.
   c. Click **Next** and click **Finish**.

For details about the reporting settings, see the VCM online help.

Standards Compliance for vCenter Operations Manager

The integration between vCenter Operations Manager and VCM includes using the VCM compliance template results to contribute to the Risk badge score in vCenter Operations Manager.

The compliance templates are included in badge mappings that are run in VCM against objects in vCenter Server instances that are managed by both VCM and vCenter Operations Manager. These objects include virtual machines, host systems, clusters, vCenter Server instances, and data stores. The compliance mapping results determine the compliance score. vCenter Operations Manager then pulls the scores into the formulas used to calculate the Risk badge scores.

When you review the standards compliance in vCenter Operations Manager, you can navigate back to VCM to view the detailed results and identify any configuration changes that you must make to bring an object that is noncompliant back to compliance.

The correct correlation of the scores requires the following conditions:

- VCM is configured to collect data from the same vCenter Server instances that are managed by vCenter Operations Manager. See "Configure vCenter Server Data Collections" on page 29.
- You must collect the required virtualization data types from the shared vCenter Server instances. The data types are vCenter Guests, vCenter Hosts, vCenter Inventory, and vCenter Settings. See "Collect vCenter Server Data" on page 32.

Configure vCenter Operations Manager Standards Compliance

Create vCenter Operations ManagerCompliance badge scores that are based on the results of VCM compliance template mapping runs. The badge scores are values that appear in vCenter Operations Manager for vCenter Server instances, datacenters, clusters, virtual machine hosts, and virtual machines managed by your vCenter Operations Manager and VCM.

Prerequisites

- Ensure that the VCM adapter is registered with the correct user account in vCenter Operations Manager. See "VCM Registration in vCenter Operations Manager for Integration" on page 73.
- Verify that VCM is configured to collect data from the same vCenter Server instances thatvCenter Operations Manager manages. See "Configure vCenter Server Data Collections" on page 29.
- Collect the required virtualization data types from the shared vCenter Server instances. The data types are vCenter Guests, vCenter Hosts, vCenter Inventory, vCenter Settings. See "Collect vCenter Server Virtual Machines Data" on page 35.
- Create compliance templates to include in the mappings. You can use Machine Group Compliance templates and Virtual Environments Compliance templates. See "Create and Run Virtual Environment Compliance Templates" on page 59.
- Review how the badge scores are calculated based on your compliance badge settings and compliance mapping options. See "Scoring Badges for vCenter Operations Manager Standards Compliance" on page 80.

Procedure

1. "Create Compliance Badge Mappings" on page 75

   Create badge mappings that contribute to the Risk badge score in vCenter Operations Manager. When you configure the mappings, you specify the templates to include, the badge to which it is assigned, and how the score is calculated.

2. "Run Compliance Badge Mappings " on page 77

   When you run the compliance badge mapping, the included templates are run against the collected data and a score is calculated based on the selected options and settings for the badge to which it is assigned.

3. "Review Mapping Scores in the Dashboard Report" on page 78

   The roll up scores appear in the Compliance Badge Rollup dashboard. Review the dashboard to ensure that the scores are calculated as expected.

4. "Schedule Compliance Badge Mapping Runs" on page 78

   Schedule the compliance badge mapping runs so that you have consistently current scores that are pulled into vCenter Operations Manager.

5. "View Compliance Badges in vCenter Operations Manager" on page 79

   The standards compliance score in VCM contributes a compliance score to the Risk badge score in vCenter Operations Manager. If the Risk score indicates distress for the object, you can view the compliance breakdown to determine which of the noncompliant templates are contributing to the score and determine what action to take to resolve the noncompliant results.

Create Compliance Badge Mappings

Create badge mappings that contribute to the Risk badge score in vCenter Operations Manager. When you configure the mappings, you specify the templates to include, the badge to which it is assigned, and how the score is calculated.

Prerequisites

- Use the Content Wizard tool to download compliance templates created by VMware,for example, the vSphere Hardening Guides and other standards. The Content Wizard is available from the Start menu on the Collector machine.
- Create compliance templates that are specific to your environment to include in the mappings. The template names should not include the | character. You can use Machine Group Compliance templates and Virtual Environments Compliance templates. See "Create and Run Virtual Environment Compliance Templates" on page 59.
- Review how the scores are calculated before configuring the mappings. See "Scoring Badges for vCenter Operations Manager Standards Compliance" on page 80.

Procedure

1. Click **Compliance**.
2. Select **vCenter Operations Manager Badge Mapping > Mappings**.
3. Click **Add**.
4. Configure the basic settings for the mapping, select the machine group or virtual objects group context, and click **Next**.

Option	Description
Name	Mapping name. Do not use the | character in the mapping name.
Description	Mapping description
Badge	Select the badge to which the mapping applies. ■ Risk - Compliance: Mapped to the vCenter Operations Manager Risk badge. ■ VCM Only: Not mapped to a vCenter Operations Manager badge. This option allows you to test mapping configurations before assigning them to vCenter Operations Manager. Does not appear in vCenter Operations Manager.

Option	Description
Roll Up Type	Select the method used to calculate how the score for the templates in a mapping is determined. Scores are always between 0 and 100. A score of 0 indicates the that all the rules are noncompliant. A score of 100 indicates that all the rules are compliant. ■ Simple Percentage: Percentage of the template results that are compliant. ■ Weighted Percentage: Percentage of the template results that are compliant where the Critical severity rule results are weighted more heavily than the Low severity rules results. ■ Simple Rule Percentage: Percentage of compliance rules in the templates that passed as compliant. If any of the results are non-compliant, the rule is noncompliant. ■ Weighted Rule Percentage: Percentage of the compliance rules in the templates where the Critical severity rule results are weighted more heavily than the Low severity rules results.
Select Group Context	Select compliance template context for which you are creating this mapping. ■ Machine Group Compliance: Select this option to add machine group templates to the mapping. The virtual machines and host machines must also be managed as virtual objects in VCM in order for the machine object IDs to correlate to the objects in vCenter Operations Manager. ■ Virtual Object Group Compliance: Select this option to add virtual environments templates to the mapping.

5. Select the Machine Group or Virtual Objects Group from which to build the mapping and click **Next**.
6. Select one or more templates to include in the mapping and click **Next**.

   The list of available templates is based on the selected machine or virtual object group. Templates used in compliance mappings should not include the | character.
7. Click **Finish**.

What to do next

Run the compliance badge mappings to determine if they are scoring as expected. See "Run Compliance Badge Mappings " on page 77.

Run Compliance Badge Mappings

When you run the compliance badge mapping, the included templates are run against the collected data and a score is calculated based on the selected options and settings for the badge to which it is assigned.

Prerequisites

- Collect the data from the machine or virtual object groups. Ensure that you collect the vCenter Guests, vCenter Hosts, vCenter Inventory, and vCenter Settings from your vCenter Server instances. See "Collect vCenter Server Data" on page 32.
- Create compliance badge mappings that include one or more templates. See "Create Compliance Badge Mappings" on page 75.

Procedure

1. Click **Compliance**.
2. Select vCenter Operations Manager **Badge Mapping > Mappings**.
3. Select a mapping and click **Run**.
4. Click **OK**.

   All templates included in the mapping are run and the score calculated. The template results are in the individual template results data grid and the score is available in the vCenter Operations Manager Compliance Rollup dashboard.

What to do next

Review the scores in the vCenter Operations Manager Compliance Rollup dashboard. See "Review Mapping Scores in the Dashboard Report" on page 78.

Review Mapping Scores in the Dashboard Report

The roll up scores appear in the Compliance Badge Rollup dashboard. Review the dashboard to ensure that the scores are calculated as expected.

The current roll up scores are also available in the Machine Group Compliance Badge Rollup Detail and Summary report.

Prerequisites

Run the Compliance Badge Mappings. See "Run Compliance Badge Mappings " on page 77.

Procedure

1. Click **Console**.
2. Select **Dashboards > Compliance > Compliance Badge Rollup**.
3. Review the scores and modify the settings as needed.

What to do next

- To ensure that the scores that are pulled into vCenter Operations Manager are always current, schedule the mappings to run at a regular time. See "Schedule Compliance Badge Mapping Runs" on page 78.
- (Optional) To change how the mappings are scored, modify the Standards Compliance Settings. Do not modify the scores unless you understand how the scores are calculated. See "Scoring Badges for vCenter Operations Manager Standards Compliance" on page 80.

Schedule Compliance Badge Mapping Runs

Schedule the compliance badge mapping runs so that you have consistently current scores that are pulled into vCenter Operations Manager.

Prerequisites

Schedule the collections for the vCenter Server instances on which you are running templates to complete the collections before you run the compliance mappings against the collected data. See "Configure vCenter Server Scheduled Collections" on page 34.

Procedure

1. Click **Administration**.
2. Select **Job Manager > Scheduled** and click **Add**.
3. Select **vCenter Operations Manager Compliance Badge Mapping Run** and click **Next**.
4. Type a name and description and click **Next**.
5. Select one mapping and click **Next**.
6. Use the scheduling options to schedule when the mapping runs.

   Schedule the job to run at the frequency at which you want refreshed results to be available to pull into vCenter Operations Manager. Schedule the compliance badge mapping to run after your scheduled collection.
7. Click **Finish**.

What to do next

View the mapped badges in vCenter Operations Manager. See "View Compliance Badges in vCenter Operations Manager" on page 79.

View Compliance Badges in vCenter Operations Manager

The standards compliance score in VCM contributes a compliance score to the Risk badge score in vCenter Operations Manager. If the Risk score indicates distress for the object, you can view the compliance breakdown to determine which of the noncompliant templates are contributing to the score and determine what action to take to resolve the noncompliant results.

Prerequisites

Verify the following requirements.

- VCM adapter is installed.
- VCM adapter is registered.
- Internet Explorer is installed.
- You have a vCenter Operations Manager user name and password from the vCenter Operations Manager administrator.

Procedure

1. In vCenter Operations Manager, select an object in the inventory pane.
2. Click **Dashboard**.
3. Click **Why is Risk {score}?** and review the Compliance score.
4. Click the Compliance badge to view the template scores associated with the overall score.
5. On the **Views** tab, the score for each template appears in the Details section.
6. To view the template results in VCM, click **View details in VCM** for the template you are investigating.
7. If necessary, copy the URL provided in the Info dialog box into the Internet Explorer address bar.

   The template results appear in VCM.

What to do next

Resolve the noncompliant results. See "Resolve Noncompliant Virtual Environments Template Results" on page 66.

Scoring Badges for vCenter Operations Manager Standards Compliance

Badge scores are values that appear in a vCenter Operations Manager Compliance badge, and which also contribute to the dashboard values for the Risk badge.

The badge score pulled into vCenter Operations Manager is a calculated value that is based on your compliance mapping options and on the compliance badge settings configured in VCM and run against collected VCM data.

A compliance mapping is one or more compliance templates that run against a machine group or virtual object group and calculate scores based on the selected options and the defined settings. When the VCM adapter is configured in vCenter Operations Manager, the score appears as a Compliance badge for the Risk badge.

Scoring Calculation Process

The badge calculations are based on mapping options and standards compliance settings. The options and the settings interact in the following workflow:

- Scoring based on mapping options.
  - Select the compliance standard badge to which the mapping contributes a score.
  - Select the roll up type that determines the initial score calculation. If you select weighted percentages, the weight values are configured in the standards compliance settings.
- Setting detail level aggregation of scores based on the standards compliance options.
- Refining the badge scores as they appear in vCenter Operations Manager using the midpoint and magnitude settings.
- Scoring the Risk badge in vCenter Operations Manager.

Scoring Based on Mapping Options

You specify the badge name and the roll up types for each mapping you create in VCM.

Standards Compliance Badges

When you create a mapping in VCM, you select the vCenter Operations Manager badge with which it is associated.

The Compliance subbadges are aligned with the following vCenter Operations Manager badge and VCM-only roll up.

- Risk - Compliance scores are included in the Risk badge.

  The Risk badge indicates potential problems that might eventually degrade the performance of the managed environment. Risk does not necessarily imply a current problem. Risk indicates problems that might require your attention in the near future, but not immediately. The overall Risk score for an object ranges between 0 (no risk) to 100 (serious risk).

Compliance mappings should include templates that evaluate your environment in a way that helps to identify performance issues. For example, you have an object setting that should be addressed if it is found to be noncompliant from the configuration standard, but it does not require immediate attention.

- VCM Only scores are available only in VCM.

  The VCM Only mapping scores are not pulled into vCenter Operations Manager. The scores are intended to provide mapping of multiple templates and scores only in VCM. For example, you can use this mapping to test a new mapping in VCMbefore you begin reporting the scores in vCenter Operations Manager.

The roll up type calculations for each badge determine the initial score.

Roll Up Types

The roll up types determine how the template results are initially scored.

When you create a compliance template, each template includes one or more rules, and you assign each rule a severity level of Low, Moderate, Important, and Critical. Each rule includes one or more individual checks that return one or more results for each check. The results for the individual checks that are made on the target machine or object determine if the object is compliant or noncompliant.

For the Weighted Percentage and Weighted Rule Percentage roll up types, you can apply a weighted value. The weighting is the value by which the result or rule is multiplied to give the different severity levels more or less weight when calculating the scores. The weighting of the severity levels is configured in the Standards Compliance Settings. The default values are Low=1, Moderate=2, Important=4, and Critical=8.

Simple Percentage is the percentage of the template results that are compliant. This option does not weight the results based on severity. For example, the simple percentage score for the results is 73. This score is calculated based on 11 compliant results out of a total of 15 results.

Table 5–1. Simple Percentage Template Results

Severity	Compliant Results	Noncompliant Results
Critical	1	4
Important	2	0
Moderate	3	0
Low	5	0
Total	11	4

Weighted Percentage is the percentage of the template results that are compliant where the Critical severity rule results are weighted more heavily than the Low severity rules results. For example, the weighted percentage score for the results is 46. This score is calculated based on a weighted value of 27 compliant results out of a total of 59 results.

Table 5–2. Weighted Percentage Template Results

Severity	Severity Weight	Compliant Results	Weighting Calculations	Weighted Compliant Results	Noncompliant Results	Weighting Calculations	Weighted Noncompliant Results
Critical	8	1	8*1=8	8	4	8*4=32	32
Important	4	2	4*2=8	8	0	4*0=0	0
Moderate	2	3	2*3=6	6	0	2*0=0	0
Low	1	5	1*5=5	5	0	1*0=0	0
Total				27			32

Simple Rule Percentage is the percentage of compliance rules in the templates that passed as compliant. If any of the results are non-compliant, the rule is non-compliant. This option does not weight the rules based on severity. For example, the simple rule percentage is 40. This score is calculated based on two compliant rules out of a total of five rules.

Table 5–3. Simple Rule Percentage Based on Template Rules

Rule/ Severity	Compliant Results	Noncompliant Results	Simple Compliant Rule	Simple Noncompliant Rule
Rule 1/ Critical	1	0	1	
Rule 2/ Important	5	6		1
Rule 3/ Important	15	1		1
Rule 4/ Moderate	1	0	1	
Rule 5/ Low	0	9		1
Total			2	3

You might choose scoring by rule rather than by results when some rule groups return significantly more rules than other rules in the same rule group. For example, a rule that checks user accounts returns one result per user account on an object, but a rule that checks a password policy returns only one result for an entire system.

Weighted Rule Percentage is the percentage of the compliance rules in the templates where the Critical severity rule are weighted more heavily than the Low severity rules. For example, the weighted rule percentage is 53. This score is calculated based on a weighted value of 10 compliant rules out of a total of 19 rules.

Table 5–4. Weighted Rule Percentage Based on Template Rules

Rule/ Severity	Severity Weight	Compliant Results	Noncompliant Results	Simple Compliant Rule	Simple Noncompliant Rule	Weighted Compliant Rule Value	Weighted Noncompliant Rule Value
Rule 1/ Critical	8	1	0	1		8	
Rule 2/ Important	4	5	6		1		4
Rule 3/ Important	4	15	1		1		4
Rule 4/ Moderate	2	1	0	1		2	
Rule 5/ Low	1	0	9		1		1
Total						10	9

Detail Level Score Aggregation

After the initial scoring, the Standards Compliance Settings determine the badge scores that are calculated for the vCenter Operations Manager badges, based first on the Detail Level aggregation, and then on the midpoint and magnitude.

The level from which to roll up the badge scores that are generated for each mapping.

Use the Standards Compliance badge settings to select the level of detail at which to roll up the scores, and the midpoint and magnitude used to adjust the scores that are reported in vCenter Operations Manager.

Table 5–5. Detail Level Score Aggregation Example Values

Templates in Mappings	Score	Results
Mapping 1 Template 1	80	10,000
Mapping 1 Template 2	50	5
Mapping 1 Template 3	100	1
Mapping 2 Template 4	30	100
Mapping 2 Template 5	75	500

- Compliance Result: To roll up at the compliance result level means that the scores for the templates assigned to the mapping, times the number of compliance results for each score divided by the total number of compliance results.

  For example, Mapping 1 has three templates using the scores and results provided in the Scoring table. The scoring is calculated as (80*10,000)+(50*5)+(100*1)/(10,000+5+1)=80, where 80 is the score.

- Template: To roll up at the template level means that each template's scores are averaged when rolled up to the badge level.

  For example, Mapping 1 has three templates using the scores provided in the Scoring table. The score is calculated as (80+50+100)/3=77, where 77 is the score.

- Mapping: To roll up at the mapping level means that the score for each mapping associated with a badge is averaged when rolled up to the badge level.

  For example, Mapping 1 and Mapping 2 are assigned to the same badge. The score is calculated as (77+53)/2=65, where 77 is the Mapping 1 average, 53 is the Mapping 2 average, and 65 is the average of the two mappings included in the badge.

Midpoint and Magnitude Score Calculations

Use midpoint and magnitude to refine how the badge scores are ultimately calculated for vCenter Operations Manager.

- Midpoint: The score that triggers the magnitude to increase or decrease the returned score.
- Magnitude: The percentage by which any score that is above or below the midpoint is calculated.

The calculation is {detail level score}-{midpoint}={difference}; {difference}*{magnitude}={adjusted magnitude factor}; {detail level score}+{adjusted magnitude factor}={adjusted score}.

Detail level scores can differ even where the midpoint and magnitude remain the same.

Table 5–6. Static Midpoint and Magnitude Values

Detail Level Score	Midpoint	Magnitude	Calculation	Adjusted Score
20	50	10	20-50=-30 -30*10%=-3 20-3=17	17
40	50	10	40-50=-10 -10*10%=-1 40-1=39	39
70	50	10	70-50=20 20*10%=2 70+2=72	72

Detail Level Score	Midpoint	Magnitude	Calculation	Adjusted Score
100	50	10	100-50=50 50*10%=5 100+5=105	100

Table 5–7. Different Magnitude Values

Detail Level Score	Midpoint	Magnitude	Calculation	Adjusted Score
70	50	20	70-50=20 20*20%=4 70+4=74	74
70	50	50	70-50=20 20*50%=10 70+10=80	80
70	50	80	70-50=20 20*80%=16 70+16=86	86

The adjusted score is the score that is pulled by the vCenter Operations Manager VCM Adapter and appears as part of the Risk badge score.

You modify the midpoint and magnitude to give the Compliance subbadge scores a stronger or weaker influence on the Risk parent badge. For example, if the compliance mappings score is configured so that it normally scores 100 and you want any deviation to clearly degrade the score, you can set the midpoint to 99 and the magnitude to a high value. The resulting adjusted score lowers the value of the compliance score and the Risk score when any noncompliance is found.

If you do not want to apply midpoint and magnitude calculations, set the magnitude to 0.

Scoring in vCenter Operations Manager

The standards compliance scores are pulled from VCM into vCenter Operations Manager and added to the Risk badge score using the following calculation:

- Risk: 100 - GeometricMean(badge|time_remaining, badge|capacity_remaining, 100 - badge|stress, badge|riskcompliance)

Auditing Security Changes in Your Environment

6

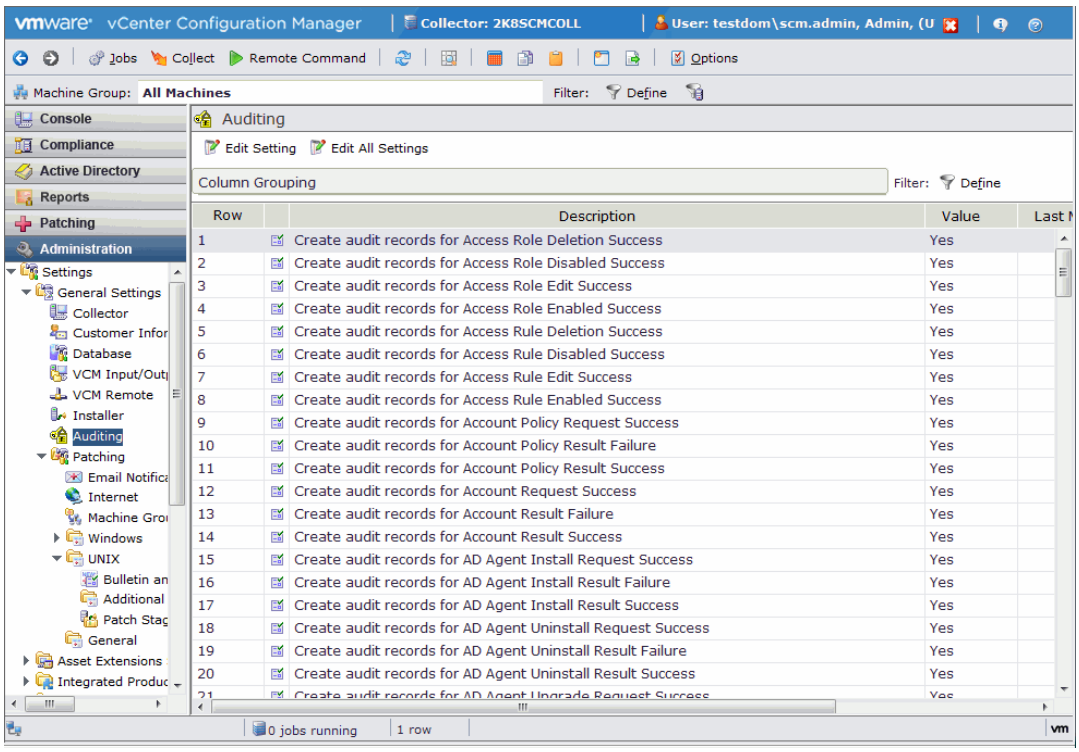
The VCM Auditing capability tracks all changes in the security aspects of VCM. Security-related events are written to the Windows Event Log, which is stored on the Collector, and is independent of the VCM application. The format of the event log prohibits any modifications to the recorded entries, which makes it a secure and tamper-proof auditing record of changes in security.

When you perform an action in VCM that affects security, and the auditing setting that corresponds to that change is enabled, the event is written to the event log.

Examples of VCM actions that cause events to be written to the event log include user log on and log off, session timeouts, changes in managing users, changes to passwords and administration settings, changes in network accounts and authority, collection requests, and service and registry changes.

VCM supports the ability to create numerous audit records.

Figure 6–1. VCM Auditing


vCenter Configuration Manager
Collector: 2K8SCMCOLL
User: testdom\scm.admin, Admin, (U
Jobs
Collect
Remote Command
Options
Machine Group: All Machines
Filter: Define
Console
Compliance
Active Directory
Reports
Patching
Administration
Settings
General Settings
Collector
Database
VCM Remote
Installer
Auditing
Patching
Windows
UNIX
General
Asset Extensions
Auditing
Edit Setting
Edit All Settings
Column Grouping
Filter: Define
Row
Description
Value
1 Create audit records for Access Role Deletion Success Yes
2 Create audit records for Access Role Disabled Success Yes
3 Create audit records for Access Role Edit Success Yes
4 Create audit records for Access Role Enabled Success Yes
5 Create audit records for Access Rule Deletion Success Yes
6 Create audit records for Access Rule Disabled Success Yes
7 Create audit records for Access Rule Edit Success Yes
8 Create audit records for Access Rule Enabled Success Yes
9 Create audit records for Account Policy Request Success Yes
10 Create audit records for Account Policy Result Failure Yes
11 Create audit records for Account Policy Result Success Yes
12 Create audit records for Account Request Success Yes
13 Create audit records for Account Result Failure Yes
14 Create audit records for Account Result Success Yes
15 Create audit records for AD Agent Install Request Success Yes
16 Create audit records for AD Agent Install Result Failure Yes
17 Create audit records for AD Agent Install Result Success Yes
18 Create audit records for AD Agent Uninstall Request Success Yes
19 Create audit records for AD Agent Uninstall Result Failure Yes
20 Create audit records for AD Agent Uninstall Result Success Yes
0 jobs running
1 row

Prerequisites

Log in as a user who has the Admin role assigned.

Procedure

1. To view the VCM Auditing settings, click **Administration**.
2. Select **Settings > General Settings > Auditing**.
3. To change an auditing setting, highlight a setting and click **Edit Setting**.

   When you change an auditing setting, the VCM Auditing data grid displays the user's name in the Last Modified By column.

What to do next

For details about the Auditing settings and the Windows Event Log, see the online help.

Configuring Windows Machines 7

To manage your virtual and physical Windows machines, you must verify domains and accounts, discover and license those machines, install the VCM Agent, and collect Windows data from those machines. You can also collect Windows Custom Information.

This chapter includes the following topics:

Configure Windows Machines 87
Windows Collection Results 94
Getting Started with Windows Custom Information 95
Prerequisites to Collect Windows Custom Information 96
Using PowerShell Scripts for WCI Collections 97
Windows Custom Information Change Management 107
Collecting Windows Custom Information 108
Create Your Own WCI PowerShell Collection Script 108
Verify that Your Custom PowerShell Script is Valid 109
Install PowerShell 110
Collect Windows Custom Information Data 110
Run the Script-Based Collection Filter 111
View Windows Custom Information Job Status Details 112
Windows Custom Information Collection Results 113
Run Windows Custom Information Reports 114
Troubleshooting Custom PowerShell Scripts 115

Configure Windows Machines

To manage Windows machines, you must configure the environmental components and machine options in VCM.

Procedure

1. Verify Available Domains

   Allow VCM access to each domain so that the VCM Collector can interact with the Windows machines in your environment.

2. Check the Network Authority

   Verify that at least one domain account with administrator privileges is available to act as a network authority account for VCM.

3. Assign Network Authority Accounts

   Select and assign the network authority account that you identified for VCM access to the Windows machines.

4. Discover Windows Machines

   In your network, identify the Windows machines that you are managing with VCM.

5. License Windows Machines

   To manage Windows machines, you must license them in VCM.

6. Install the VCM Windows Agent on Your Windows Machines

   Install the VCM Windows Agent on each Windows machine so that you can collect data and manage the virtual or physical machines.

7. Collect Windows Data

   Start managing the Windows machines by performing an initial collection, which adds Windows machine data to VCM.

Continuous Windows machine management is based on the latest data you collect from target machines. You can view data and run actions, such as reports or compliance, based on the collected data. See "Windows Collection Results" on page 94.

Verify Available Domains

Allow VCM access to each domain so that the VCM Collector can interact with the Windows machines in your environment.

During installation, VCM discovered all domains to which the network authority account had access. If the Windows machines belong to a domain that is not listed, you must add that domain manually.

Prerequisites

Verify that you have the fully-qualified names of the domains to manage.

Procedure

1. Click **Administration**.
2. Select **Settings > Network Authority > Available Domains**.
3. If the domain does not appear Available Domains view, add the domain.
   a. Click **Add**.
   b. Type the domain name and select the domain type as **NetBios** or **AD**, depending on your domain.
   c. Click **OK**.
4. Verify that the domain appears in the data grid.

What to do next

Verify that a network authority account is available and create other necessary domain accounts. See "Check the Network Authority" on page 89.

Check the Network Authority

Verify that at least one domain account with administrator privileges is available to act as a network authority account for VCM.

Although you specified an initial default network authority account when you installed VCM, you can add different administrator accounts if you do not assign the default account.

Prerequisites

Verify the presence of domains. See "Verify Available Domains" on page 88.

Procedure

1. Click **Administration**.
2. Select **Settings > Network Authority > Available Accounts**.
3. To add a new domain account, click **Add**.
4. Type the domain name, user name, and password, and click **Next**.
5. Click **Finish** to add the account.

What to do next

Assign the network authority account to the domain so that VCM can access the Windows machines in the domain. See "Assign Network Authority Accounts" on page 89.

Assign Network Authority Accounts

Select and assign the network authority account that you identified for VCM access to the Windows machines.

You can assign a single account to all domains and machine groups, or assign a unique account or multiple accounts to each domain and machine group.

In this procedure, NetBios is used as the example.

Prerequisites

Verify or add the necessary network authority account. See "Check the Network Authority" on page 89.

Procedure

1. Click **Administration**.
2. Select **Settings > Network Authority > Assigned Accounts > By Domain > NetBios**.
3. Select an assigned account.
4. Click **Edit Assigned Accounts**.
5. Select the account to receive authority to the domain and click **Next**.
6. Confirm the accounts to include in the authority list for the domain and click **Finish**.

What to do next

Discover the Windows machines in your environment. See "Discover Windows Machines" on page 90.

Discover Windows Machines

In your network, identify the Windows machines that you are managing with VCM.

To discover the available Windows machines, VCM uses general discovery rules to identify many Windows machines or uses specific discovery rules to identify particular Windows machines.

The time required to perform an initial discovery depends on the size and composition of your network. If all Windows machines are not available during initial discovery, such as systems that are disconnected from the network, the first discovery will not find all Windows machines. If the discovery does not identify all Windows machines, you might need to run additional discoveries after the other Windows machines become available.

NOTE You can use the Discovered Machines Import Tool (DMIT), which imports machines discovered by the Network Mapper (Nmap), to import many physical and virtual machines at one time into the VCM database. Download DMIT from the VMware Web site.

The following procedure is based on Active Directory.

Prerequisites

Assign a Network Authority Account that VCM can use for access. See "Assign Network Authority Accounts" on page 89.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Discovery Rules**.
3. Click **Add** to create a discovery rule.
4. On the Discovery Rules page, type a name and description and click **Next**.
5. On the Discovery Method page, select **By Active Directory** and click **Next**.
6. On the AD Domain page, specify the AD Domain, select **Discover machines only from the selected domain**, and click **Next**.
7. On the Discovery Filters page, select **Discover all machines in <domain_name> Domain**.
8. (Optional) Create a filter to discover Windows machines based on a limited criteria and click **Next**.
9. On the Important page, click **Yes** and click **Finish**.

   To avoid exceeding your license count, do not select **License and Install Agent on Discovered Machines**.
10. On the toolbar, click **Jobs** to track current discovery job status.

What to do next

- Verify that the jobs finished running. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.
- Verify that the Windows machines are available. Click **Administration** and select **Machines Manager > Available Machines**.
- License the Windows machines in your environment. See "License Windows Machines" on page 90.

License Windows Machines

To manage Windows machines, you must license them in VCM.

The number of discovered Windows, UNIX, or Linux machines might exceed the number of your available licenses. If that happens, the number available goes negative and appears in red to indicate that you do not have enough licenses.

For servers and workstations, exceeding the limit on your license key produces warnings but does not restrict VCM operation. License key counts that are over the limit are recorded and maintained for auditing purposes. Suite license keys support unlimited licenses, provided that the suite edition includes VCM and the component that you are managing is part of the suite. If a component is not part of the suite, it counts against the nonsuite server or workstation key.

Prerequisites

Verify that the Windows machines you license are listed with a machine type of workstation or server in the Available Machines node. If the discovered or added type is not workstation or server, VCM cannot license the machines.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Available Machines**.
3. Select the Windows machines to license.
4. Click **License**.
5. Verify that the Windows machines to license appear in the Selected list.

   Use the arrows to move the Windows machines.
6. Click **Next** to view your Product License Details.

   The licensed Windows machine count increases by the number of licensed machines.
7. Click **Next**.

   VCM confirms that the licenses you requested will be applied to the selected Windows machines.
8. Click **Finish**.

What to do next

Install the Windows Agent. See "Install the VCM Windows Agent on Your Windows Machines" on page 91

Install the VCM Windows Agent on Your Windows Machines

Install the VCM Windows Agent on each Windows machine so that you can collect data and manage the virtual or physical machines.

Before you can collect data from Windows machines, you must install the VCM Windows Agent on the licensed Windows machines in your environment to enable communication between the Collector and the target machines.

You can use VCM to install the Agent or you can install the Agent manually. This procedure uses VCM to install the Agent. For information about manually installing the Agent see the online Help.

The Agent is installed on Collector when you install VCM, and locked. It cannot be unlocked, uninstalled, or upgraded.

Locking the VCM Agent on VCM managed machines is typically done in environments that have multiple VCM Collectors, to help prevent these Agents from being unintentionally upgraded or removed. The VCM Agent on the VCM Collector is locked, because it is installed as part of the VCM installation and is required for VCM Collector operations. The version of the VCM Agent on the Collector must also match the version of VCM installed.

Use the UNLOCK option only when you intend to upgrade or uninstall a locked Agent on a VCM managed machine. Never use the UNLOCK option on the VCM Collector. If the VCM Agent is uninstalled from the Collector, the Collector service cannot run. If the VCM Agent is accidentally uninstalled from a Collector, you must reinstall it and restart the Collector service to re-enable the Collector functionality. If the VCM Agent is unintentionally reinstalled on a Collector, you must restart the Collector service.

Standardized Windows configurations such as Federal Desktop Core Configuration (FDCC) or United States Government Configuration Baseline (USGCB) include strict security group policy settings. The **Windows Firewall: Do not Allow Exceptions** group policy configures Windows Firewall to block all unsolicited incoming messages, including configured exceptions. This setting overrides all configured exceptions. For VCM to communicate properly with the VCM Agent on managed machines in strict, secure environments, disable the **Windows Firewall: Do not Allow Exceptions** group policy on the managed machines. For more information, see support.microsoft.com.

Prerequisites

- License the Windows machines on which you install the Agent. See "License Windows Machines" on page 90.
- Verify that you know the communication protocols and ports that are used by the Collector and the Agents.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed Windows Machines**.
3. In the data grid, select one or more Windows machines on which to install the Agent and click **Install**.
4. On the Machines page, verify that the target machines appear in the Selected list and click **Next**.
5. On the Install Options page, select the installation options and click **Next**.

Option	Description
Share	Location to install the Agent. The default location is `ADMIN$`.
Path	Path for the Agent files. The default path includes `CMAgent`.
Install From	VCM Collector from which to install the Agent.
DCOM	Communication protocol for the Agent. The default setting is DCOM.
HTTP	Secure communication protocol for the Agent. Use HTTP, which installs the HTTP Listener on the target machine and configures it to listen on the designated port.
Port	Designated port for the HTTP Listener.

Option	Description
Install using a proxy server	For Windows Proxies and Windows Agents only. If the target machine is separated from the Collector by a proxy server, this option instructs the installation process to check for available proxy servers.
Lock the machine after installation	Ensures that VCM will not uninstall the Agent or replace it with a different version.
Reinstall Agent	Overwrites an installed Agent.

6. On the Schedule page, select **Run Action now** and click **Next**.

   You can schedule subsequent Agent installations to run later.

7. Review the summary information and click **Finish**.

What to do next

- Verify that the jobs finished running. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.
- Collect Windows data from VCM managed machines in your environment. See "Collect Windows Data" on page 93.

Locate the Enterprise Certificate

Locate the Enterprise Certificate before you install the VCM Agent on the managed Windows machine. VCM must access the Enterprise Certificate during the Agent installation.

If your Collector is operating in a full Public Key Infrastructure (PKI), and the target machine can validate the Collector root certificate (Enterprise Certificate), the `.pem` file is not required.

Procedure

1. Locate the Enterprise Certificate `.pem` file in the Collector's `c:\Program Files (x86)\VMware\VCM\CollectorData` folder.
2. If the certificate files are not in the default location, you must confirm the path to the files.
   a. Click **Administration**.
   b. Select **Settings > General Settings > Collector**.
   c. Select **Root directory for all collector files**.
   d. Confirm the file path in the **Value** column.

Collect Windows Data

Start managing the Windows machines by performing an initial collection, which adds Windows machine data to VCM.

Use the default filter set to collect a general view of the Windows machines in your environment. The first time that you use the default filter to collect data, the Windows Agent returns all of the data specified in the filter and stores the data in the VCM database. All subsequent collections will return a delta against the data previously collected.

A delta collection includes only the differences between the data on the target machine and the data stored in the VCM database. If you need a full collection, you can specify that VCM collect all data again. A full collection can take a significant amount of time depending on the number of VCM managed Windows machines from which you are collecting.

When you perform a full collection from your entire environment, run the collection during nonworking hours so that users do not notice any performance impact on managed machines. After the initial collection is finished, subsequent delta collections will most likely not impact performance.

Prerequisites

- Collect the Accounts and Groups data types from the primary domain controller (PDC) in each domain to increase the performance of initial collections that require a SID lookup.
- To collect data from Windows XP SP2 or Vista machines that use DCOM communication, you must enable ICMP pings in the firewall settings or disable ICMP pings in VCM.
- Verify that DCOM is enabled on the managed machine. Run `dcomcnfg` and select **Enable Distributed COM on this computer**.

Procedure

1. On the VCM toolbar, click **Collect**.
2. On the Collection Type page, select and click **OK**.
3. On the Machines page, select the Windows machines from which to collect data and click **Next**.

   To move all visible Windows machines to the selection window, 500 at a time, use the double arrow.
4. On the Data Types page, configure the collection and click **Next**.
   a. Expand Windows and select the data types.

      At a minimum, you must collect **Machines** data. If you are managing data using compliance, change, or running reports, you must collect the data types that are included in the other actions or that you want to view in the appropriate data grids.

   b. Select **Use default filters**.
5. On the Important page, resolve any conflicts and click **Finish**.
6. Click **Administration** and select **Job Manager > History > Instant Collections > Past 24 Hours** to determine if the collection finished.

   The amount of time the collection requires is determined by the number of machines and network connectivity.

What to do next

- Verify that the jobs finished running. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.
- Review the collection results. See "Windows Collection Results" on page 94.

Windows Collection Results

Continuous Windows machine management is based on the latest data that you collect from target machines. You can view data and run actions, such as reports or compliance, based on the collected data.

Windows data appears in VCM and is available for several management actions, including Console dashboards and reports, Compliance views, and VCM Patching. The displayed data is only as current as the last time you collected the data.

After the initial discovery is finished, perform a weekly discovery to update the list of available Windows machines. To schedule a VCM discovery job, click **Administration**, select **Job Manager > Scheduled**, and follow the wizard.

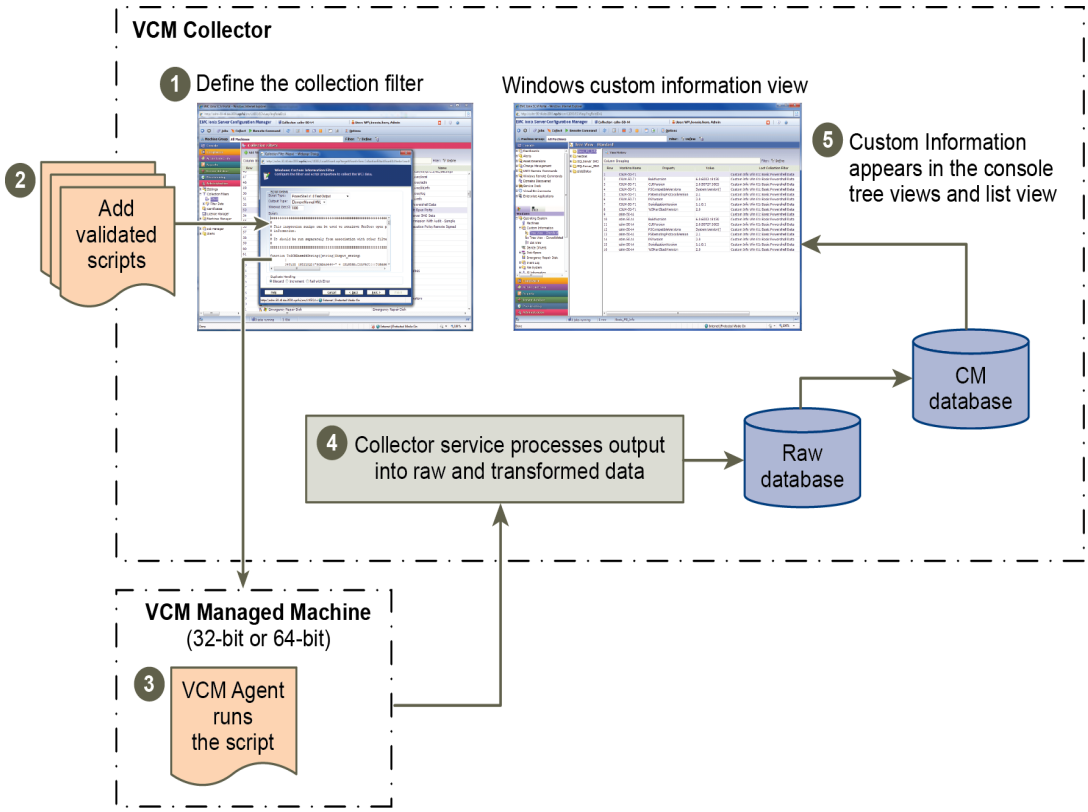
Option	Description
Console	Displays dashboards and reports based on collected data. Use the Console to view data that is relevant to day-to-day operations, troubleshooting, and analysis. ■ To view the dashboards, click **Console** and select **Dashboards > Windows > Operating Systems**. ■ To view the summary reports, click **Console** and select **Windows > Operating System > Machines**. You can view the data in a summary report or data grid format.
Compliance	Determines if the data collected from VCM managed Windows machines meets specified compliance values, and allows you to run compliance remediation actions. ■ To run a compliance check, click **Compliance** and select **Machine Group Compliance**. ■ To create rule groups, rules, filters, and templates, see the online help.
Reports	Runs preconfigured reports or you can create custom reports. VCM runs reports against the latest collected data. Depending on the data volume or complexity of the requested report, it might take time to generate the report. You can also schedule and disseminate reports. ■ To use the reporting options, click **Reports** and select **Machine Group Reports > Windows**.
Patching	Assesses target machines to determine if the patching status of the Windows machines is up-to-date. You can install the latest patches on target machines. ■ To assess and patch Windows machines, click **Patching** and select **Windows**. ■ To run assessments and patch your Windows machines, see the online help.

Getting Started with Windows Custom Information

Windows Custom Information (WCI) is data collected from VCM managed machines that is created by PowerShell or Python scripts. WCI supplements and extends the data collected by VCM from managed Windows machines using other VCM data types.

You can create or modify WCI scripts to collect almost any data type that is accessible from VCM managed machines. VCM supports PowerShell and Python scripting, and XML output to collect Windows Custom Information.

Figure 7–1. Windows Custom Information Collection Process


VCM Collector
1 Define the collection filter
Windows custom information view
2 Add validated scripts
5 Custom Information appears in the console tree views and list view
CM database
4 Collector service processes output into raw and transformed data
Raw database
VCM Managed Machine
(32-bit or 64-bit)
3 VCM Agent runs the script

To extend the data collected by VCM from managed Windows machines using other VCM data types, collect Windows Custom Information. The example used to get you started collecting WCI data is for Powershell. Follow the same basic procedures to configure and run Python scripts.

Configure the prerequisites and create and validate your script.

Prerequisites

To collect Windows Custom Information from VCM managed machines, you must configure the prerequisites. See "Prerequisites to Collect Windows Custom Information" on page 96.

Procedure

- "Collecting Windows Custom Information" on page 108

  To collect Windows Custom Information (WCI) using script-based filters, you create and verify your custom PowerShell scripts, install PowerShell on the VCM managed machines, and use VCM to collect the WCI data.

Prerequisites to Collect Windows Custom Information

To collect Windows Custom Information from VCM managed machines, you must configure the prerequisites.

These prerequisites use PoweShell as the example script. VCM supports PowerShell and Python scripts to configure WCI collections.

Prerequisites

- Write your own PowerShell script to return data in a VCM compatible, element-normal XML format, or obtain PowerShell scripts from VMware Professional Services or another source. See "Using PowerShell Scripts for WCI Collections" on page 97.
- Understand the script signing policies if you use PowerShell 2.0. See "PowerShell Script Signing Policies" on page 101.
- Set the PowerShell execution policy on the VCM managed machine. See "Built-In PowerShell Policy Settings" on page 102.
- Understand how to write and run PowerShell scripts. See "References on PowerShell and Script Signing" on page 102.
- Verify that your PowerShell script is accessible when you paste the script content into the Script area of the collection filter on the VCM Collector.
- Confirm that the VCM Collector includes PowerShell 2.0 if the Collector is a client for WCI collections.
- Understand how VCM manages Windows Custom Information data changes. See "Windows Custom Information Change Management" on page 107.
- Confirm that PowerShell 2.0 is installed on each VCM managed machine that will be used for WCI collections. See "Install PowerShell" on page 110.
- Upgrade older VCM Agents on the VCM managed machines from which you collect Windows Custom Information, and then install the VCM 5.3 Agent or later on these machines.
- Confirm or update the Agent Thread Administration settings on the VCM Collector. The default value is set to below normal thread priority, and the Agent Data Retention default is set to a 15-day change log.

Using PowerShell Scripts for WCI Collections

Windows Custom Information (WCI) uses PowerShell as the scripting engine and the element-normal XML format as the output that is inserted into the VCM database.

WCI supports PowerShell 2.0 and works with later versions of PowerShell.

- PowerShell 2.0 is the base requirement for WCI in VCM because of its ability to set the execution policy at the process level.
- You can run WCI PowerShell collection scripts against Windows machines that have PowerShell 1.0 installed if needed, although this usage is not supported or tested. If the collection scripts do not use PowerShell 2.0 commands, your WCI filters that use the in-line method to pass a WCI script to PowerShell will operate correctly.

The WCI data type uses extensions to the VCM Windows Agent. The extensions allow the Agent to invoke PowerShell scripts. Using the script-based collection filter, VCM passes the PowerShell scripts to a VCM managed machine, and the VCM Agent parses the resulting XML output. The default WCI filter returns the PowerShell version information from the managed machines.

WCI data type extensions are flexible because they use filter parameters that the command line uses to invoke the scripting engine. The WCI extensions use a COM class name to specify the parser required for the Agent to parse the script output, and allow new types of parsers to be added at the Agent. This approach extends the support of multiple scripting engines, languages, and output formats.

Guidelines in PowerShell Scripting for WCI

When you develop custom PowerShell scripts to collect the Windows Custom Information (WCI) data type from VCM managed Windows machines, follow these guidelines.

- Make XML element names unique at the same level.

  For example, you can specify two child nodes that are not siblings.

- Make attributes unique at the same level.
- Use unique XML element names to generate valid VCM XML. The XML elements are code blocks that include the element's start and end tags. The element can contain other elements, text, attributes, or a combination of them.
- Use repeatable identifiers to prevent false indications of changes at the Collector. If your element labels (identifiers) are not the same for every collection of the same item, you will see false additions, changes, and deletions in the VCM change log.
- Confirm that the script returns valid XML element names and attribute names.

  If the data to be returned is an element name or an attribute name that is not valid for XML, you can encode the name using the [`ToCMBase64String`] function. A VCM Collector job, called the inserter, is executed during each collection. The inserter recognizes the names that are encoded with this function and decodes them in the raw insertion process.

  The inserter parses the resulting XML file and inserts the data into a new raw database table named VCM_Raw by default. The XML process transforms the raw data into data that appears in VCM.

  The function is defined as follows.

  ```
  function ToCMBase64String([string]$input_string)
  {
  return [string]("cmbase64-" +
  [System.Convert]::ToBase64String([System.Text.Encoding]::UNICODE.GetBytes
  ($input_string))).replace("=","-")
  }
  ```

- Include a comment block and configurable parameter entries near the start of the script so that when you clone a WCI collection filter you can see the parameters and set them when you edit the collection filter. To view and edit the collection filters, click **Administration** and select **Collection Filters > Filters**.
- Redirect any variable declarations in the script to out-null, along with any other tasks that generate output that is not part of the XML result set. For example, you can use the following command.

  ```
  [reflection.assembly]::LoadWithPartialName("Microsoft.SqlServer.Smo") > out-
  null
  ```

- Do not include any formatting, white space, carriage returns, or line feeds at the end of elements, nodes, or attributes.

Challenges in PowerShell Scripting for WCI

When you develop custom collection scripts, understand the challenges that you might encounter while scripting in PowerShell to collect the Windows Custom Information (WCI) data type from VCM managed Windows machines.

PowerShell scripts can use the split method of PowerShell strings, which separates the columns of the rows into separate values in arrays. For example, Windows provides the `schtasks.exe` utility to manage scheduled tasks on a local or remote computer and report on the scheduled tasks.

The split method of PowerShell strings in the `$schtasks` script separates the columns of the `$schtasks` rows into separate values in arrays.

- Column names row provides the names to use for attributes.
- Corresponding data from the scheduled task rows provides the values to use for these attributes.

The top-level name of `<schtasks>` is an arbitrary name that you apply to distinguish the results of this script from other results. The XML script returns the parsed data, which resembles the following structure.

```
<schtasks>
     <taskname1>
          <attribute1>Value1</attribute1>
          <attribute2>Value2</attribute2>
     </taskname1>
     <taskname2>
          <attribute1>Value1</attribute1>
          <attribute2>Value2</attribute2>
     </taskname2>
</schtasks>
```

The returned data can include the following problems with content.

- White space, such as tabs or spaces, is not allowed in returned data.
- Column names include spaces.
- Specific task entries do not include a unique and repeatable identifier.
- Values can contain XML syntax in functions, which you must enclose in CDATA.

Column Names Include Spaces

Running the `schtasks` command without any options displays a column name of `Next Run Time`. Because this name includes spaces, you cannot use it as an attribute name in an XML document. Running the `schtasks` command verbosely generates other column names that include spaces. Although you cannot use these invalid names as attribute names, you can preserve the names by using VCM encoding standards.

To preserve these column names in the form that `schtasks` returns and allow for XML handling, VCM encodes the column names with the `ToCMBase64String` function. To create a valid XML form of an element name or attribute name, this function uses Unicode Base64 encoding and character substitution, such as using a dash instead of an equal sign, as shown in the following example.

```
function ToCMBase64String([string]$input_string)
     {
     return [string]("cmbase64-" +
     [System.Convert]::ToBase64String([System.Text.Encoding]::
     UNICODE.GetBytes($input_string))).replace("=","-")
     }
```

Using this function corrects the invalid column name data.

VCM prefaces the string with `cmbase64-` so that the VCM inserter can decode the data and load the decoded data into the VCM database.

The valid XML appears as follows.

```
<cmbase64-TgBlAHgAdAAgAFIAdQBuACAAVABpAG0AZQA->
12:32:00, 5/26/2010
</cmbase64-TgBlAHgAdAAgAFIAdQBuACAAVABpAG0AZQA->
```

Invalid XML omits the encoding function as follows.

```
<Next Run Time>
12:32:00, 5/26/2010
</Next Run Time>
```

Task Entries Do Not Include a Unique and Repeatable Identifier

Use repeatable identifiers to prevent false indications of changes at the Collector. If your element labels (identifiers) are not the same for every collection of the same item, you will see false additions, changes, and deletions in the VCM change log.

The Windows `schtasks` command does not include a unique and repeatable identifier for specific task entries. Because unique element names are a requirement for valid VCM XML and repeatable identifiers help prevent false indications of changes at the VCM Collector, you must code the task names correctly in your script.

To create unique and repeatable element names, create a task entry name based on a hash of the data in the row. You can use this method for data that does not have a name-type attribute, where the task name exists but is not guaranteed to be unique. When the task name is user-friendly and useful, you must attempt to preserve the name and use it in the collection script.

To preserve the user-friendly name, use the task name as the element name for the task rows. When you create a collection filter that uses your script, you must select the incremental duplicate handling option so that the collection process includes an incremental entry in the list of entries where the same task name appears multiple times.

For example, in a sample test environment, many Windows machines had more than one task named `GoogleUpdateTaskMachineCore`. A PowerShell script can label the rows as Task1, Task2, and so on. If you delete Task1, Task2 becomes Task1, and VCM displays multiple change details for Task1, such as the command line and the next run time. This report would be incorrect because even though Task 1 would have changed place in the sequence, the task would not have changed.

The task names are labeled accordingly.

- The first task entry is labeled `GoogleUpdateTaskMachineCore`.
- The second task entry is labeled `GoogleUpdateTaskMachineCore_1`.

Because task names can contain characters that are not valid in XML element names, VCM encodes the task names with the `ToCMBase64String` function. If you reorder the list of tasks whose names are identical, VCM can still report extra changes. For this reason, require the VCM user interface to display the friendly task names.

Enclose Values that Can Contain XML Syntax in CDATA

When you develop your custom PowerShell scripts to collect the Windows Custom Information data type from VCM managed Windows machines, you must use CDATA to enclose values that contain XML syntax.

For example:

```
function wrapInCDATA( [string]$input_string)
{
[string]$wrappedInCDATA | out-null
if ( $input_string.Length -gt 0 )
{
$wrappedInCDATA = ("<!" + "[CDATA" + "[" + $input_string + ("]" + "]" + ">")
)
}
return $wrappedInCDATA
}
```

PowerShell Script Signing Policies

With PowerShell 2.0 you can set the script signing policies at the machine, user, and process levels. The process level runs a single execution of `powershell.exe`.

In VCM, Windows Custom Information (WCI) uses script type information in the collection filter to determine how to execute PowerShell and how to pass the script to it.

Use the following methods to pass a WCI script to PowerShell.

- **In-line:** The default WCI filter uses an in-line script to collect basic information about the PowerShell version, .NET version, and execution policy settings. The in-line option requires a collection script that is represented as a single line of PowerShell code. Because the filter runs an in-line script on the PowerShell command line, instead of using a file, the execution policy does not apply.
- **Script file:** For script-based filters in WCI, the default script type command line includes options to set the process-level execution policy to Remote Signed. The script requires that the execution policy be set to Remote Signed at the most restrictive level because the script runs from a file that resides locally on the VCM managed Windows machine. For WCI, VCM can execute collection scripts on managed machines where the machine and user level signing policies are set to any level, without requiring you to change the setting.

Built-In PowerShell Policy Settings

Before you use the WCI collection filter to run file-based PowerShell scripts on the VCM Collector and your VCM managed machines, you must change the execution policy on the VCM managed machines.

PowerShell contains built-in execution policies that limit its use as an attack vector. By default, the execution policy is set to Restricted, which is the primary policy for script execution.

The following policy settings apply to PowerShell scripts.

- **AllSigned:** PowerShell scripts must be signed by a verifiable certificate from the Software Publishing Certificate store. The typical file extension is `.ps1`. For signed scripts, you can set the execution policy to **All Signed**. You must sign the scripts and distribute the appropriate certificates before you collect WCI data.
- **RemoteSigned:** A verifiable certificate must sign any PowerShell script that you download from the Internet using a supported browser such as Internet Explorer. Script files that are not required to be signed are scripts that you create locally or scripts that you download using a method that does not support flagging the file source. For unsigned scripts, you must set the execution policy to the most restrictive level of **Remote Signed**. You can set the policy directly by using a Group Policy Object (GPO) with a VCM remote command. You can use a registry change action or enforceable compliance. For example:

  ```
  HKLM\Software\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
  "ExecutionPolicy"="RemoteSigned"
  ```

- **Unrestricted:** All PowerShell script files run regardless of whether they are signed by a verifiable certificate.
- **Restricted:** You can use PowerShell interactively or to run commands directly from the command line. This setting is the default.

References on PowerShell and Script Signing

For information about Windows PowerShell and script signing policies, see the Microsoft Web site.

Create an Example PowerShell Script for Scheduled Tasks

Use a custom PowerShell script to collect Windows Custom Information (WCI) data from VCM managed Windows machines. With this example, you can learn how to use PowerShell scripts to collect WCI data for scheduled tasks.

Windows provides the `schtasks.exe` utility to report on scheduled tasks that you create in the Task Scheduler user interface or by using the `AT` command. The `schtasks.exe` utility enables you to manage scheduled tasks on a local or remote computer and to report on the scheduled tasks.

The `schtasks` command returns basic information about scheduled tasks. The data returned by `schtasks` includes multiple rows. PowerShell structures the `$schtasks` variable in an array. For example, `$schtasks[0]` represents the first row. To view the result set, use `$schtasks[n]`, which displays the following status:

- `$schtasks[0]` is blank.
- `$schtasks[1]` contains column names.
- `$schtasks[2]` is the first row of task data.

Prerequisites

- Review the guidelines to create PowerShell scripts for WCI collections, and understand the challenges in PowerShell scripting. See "Guidelines in PowerShell Scripting for WCI" on page 98.
- Understand how to write and run PowerShell scripts. See "References on PowerShell and Script Signing" on page 102.

Procedure

1. On your VCM managed Windows machine, click **Start**.
2. Select **All Programs > Accessories > Windows PowerShell**.
   - On a 64-bit Windows machine, select **Windows PowerShell (x86)** to run the 32-bit version of PowerShell.
   - On a 32-bit Windows machine, select **Windows PowerShell**.
3. Run the command to set the source of data for the collection script.

   ```
   $schtasks = schtasks /query /v /fo:csv
   ```

Option	Description
`/query /v`	Displays additional information about scheduled tasks. Verbose formatting is difficult for automated processing.
`schtasks /query /v /fo:csv`	Displays verbose task output and sets the source of data for the collection script to a comma-separated value (csv) result set.
`schtasks /query /?`	Displays additional command options.

4. To return the data to the VCM Collector, parse the data into a structure that is compatible with the VCM XML format.

   The sample script parses the data as shown in the following code.

   ```
   ################################################################################
   ###

   #

   # This inspection script can be used to retrieve scheduled tasks
   information

   # for tasks created through the Scheduler UI or through the AT command.

   #

   ################################################################################
   ###
   ```

```
function ToCMBase64String([string]$input_string)
     {
return [string]("cmbase64-" + [System.Convert]::ToBase64String
([System.Text.Encoding]::UNICODE.GetBytes
($input_string))).replace("=","-")
     }
#########################################################################
###
[string]$cihash | out-null
#create a hashtable to check for duplicate rows
$hasharray = @{}
$clTasks = ("<Scheduled_Tasks>")
$split = [char]3
$schtasks = schtasks /query /v /fo:csv
if ($schtasks.count -gt 1)
     {
     #depending on OS, the first row may be blank
     #use $k to determine whether to start at the first or second row
     if ($schtasks[0] -eq "")
          {
          $k = 1
          }
     else
          {
          $k = 0
          }
     $cols = $schtasks[$k].substring(1,$schtasks[$k].length-2).replace
     ("""","""",$split).split($split)
     #find the HostName and TaskName columns
     $hostcol = -1
     $namecol = -1
     $j = 0
     while (($j -lt $cols.count) -and (($hostcol -eq -1) -or ($namecol -eq
     -1)))
          {
          if (([string]$cols[$j]).toupper() -eq "HOSTNAME")
```

```
            {
            $hostcol = $j++
            }
            else
                  {
                  if (([string]$cols[$j]).toupper() -eq "TASKNAME")
                        {
                        $namecol = $j++
                        }
                  else
                        {
                        $j++
                        }
                  }
      }
#save first column name, to check for repeated column rows
$firstcol = $cols[0]
#encode each column name
for ($j=0;$j -lt $cols.count;$j++)
      {
      $cols[$j] = [string](ToCMBase64String($cols[$j]))
      }
#loop through each row
#start at $k+1, because the first row may blank, and the first
populated row is column names
for ($i=$k+1;$i -lt $schtasks.count;$i++)
      {
      #make sure this is a data row
      $row = ([string]($schtasks[$i])).trim()
      if ($row.contains("""","""))
            {
            #split the row
            $task = $schtasks[$i].substring(1,$schtasks[$i].length-
            2).replace("""","""",$split).split($split)
            #some operating systems will return columns multiple times
            in the result set
```

```
if ($task[0] -ne $firstcol)
     {
     #if we did not find a TaskName column, just tag each
     row as Task-n
     if ($namecol -gt -1)
          {
          $clTasks += "<" + [string](ToCMBase64String($task
          [$namecol])) + ">"
          }
     else
          {
          $clTasks += ("<Task-" + ([string]($i-1)) + ">")
          }
     for ($j=0;$j -lt $task.count;$j++)
          {
          #skip the hostname field, since we are doing a
          local inspection
          if (-not($j -eq $hostcol))
               {
               $clTasks += ("<" + $cols[$j] + ">")
               $clTasks += $task[$j]
               $clTasks += ("</" + $cols[$j] + ">")
               }
          }
     #if we did not find a TaskName column, just tag each
     row as Task-n
     if ($namecol -gt -1)
          {
          $clTasks += "</" + [string](ToCMBase64String
          ($task[$namecol])) + ">"
          }
     else
          {
          $clTasks += ("</Task-" + ([string]($i-1)) + ">")
          }
     } #end data row that is not columns repeated
} #end data row
```

```
            } #end row loop
        }


    $clTasks += ("</Scheduled_Tasks>")
    write-host $clTasks
```

5. After you generate your PowerShell script, perform the following steps:
   - Build a collection filter in VCM.
   - Paste the content of your script into the collection filter.
   - Collect data using the script-based collection filter.

     To view the collected WCI data in VCM, click **Console** and select **Windows Operating System > Custom Information > List View**.

What to do next

Develop your own custom PowerShell script. See "Create Your Own WCI PowerShell Collection Script" on page 108.

Windows Custom Information Change Management

VCM manages Windows Custom Information (WCI) data changes on a per-filter basis on VCM managed Windows machines. When multiple filters return data using the same top-level XML element name, each filter applies unique change detection.

When you use multiple collection filters to collect WCI data, follow these guidelines.

- Create filters that collect data in a parallel manner. Use one filter to collect data from `C:\` and another filter to collect data from `C:\Windows`. Use a separate filter to collect data from `C:\Windows` with audit information and another filter to collect data from `C:\Windows` without audit information.

  When you use filters in an unparallel way, every time the file system updates to add a new file or remove an existing file, both filters generate "new file" and "deleted file" events, which causes overlap of the data.
- Use one filter to collect data from NetStat.
- Use multiple filters to collect data from the NTFS file system.

  For example, use one filter to collect data in `C:\`, and another filter to collect data in `C:\Windows\System`. These collections merge under the top-level element `NTFSDirectory` without overlap, because each filter collects separate parts of the file structure and avoids extra change reporting.
- Do not create filters that overlap collected WCI data. Overlap can occur if you use filters that do not collect data in a parallel manner.
- Do not use multiple filters to collect the same data for NetStat Open Ports.

  When the filters return data under the top-level element name and a managed machine starts to listen on port 80, each filter initially reports the data as a newly created value, which causes overlap of the data reported.
- Do not create two filters to collect data on the File Permission With Audit data type from different parts of a managed machine's file system.

Collecting Windows Custom Information

To collect Windows Custom Information (WCI) using script-based filters, you create and verify your custom PowerShell scripts, install PowerShell on the VCM managed machines, and use VCM to collect the WCI data.

VCM supports PowerShell and Python to create WCI collections. These procedures use PowerShell as the example.

Procedure

1. "Create Your Own WCI PowerShell Collection Script" on page 108

   Create or modify your Windows Custom Information (WCI) scripts to collect almost any data type that is accessible from VCM managed Windows machines. To return data in a VCM compatible, element-normal XML format, you create your own PowerShell script or obtain PowerShell scripts from VMware Professional Services or another source and modify them for your own collections.

2. "Verify that Your Custom PowerShell Script is Valid" on page 109

   Verify that your PowerShell script adheres to valid XML before you use the script to collect Windows Custom Information (WCI) from VCM managed machines.

3. "Install PowerShell" on page 110

   Verify that PowerShell 2.0 is installed on each VCM managed Windows machine used to collect Windows Custom Information (WCI).

4. "Collect Windows Custom Information Data" on page 110

   Use the Windows Custom Information (WCI) data type to perform user-defined, script-based collections on your VCM managed machines. To collect the custom data, you build a collection filter that includes a script with parameters to run the script and process the results.

5. "View Windows Custom Information Job Status Details" on page 112

   When you run Windows Custom Information (WCI) collection filter scripts, VCM captures detailed information and displays status about exit codes and standard error output for each job that processed the script or filter. You can view the job status details in Job Manager.

6. "Windows Custom Information Collection Results" on page 113

   Examine the results of your Windows Custom Information (WCI) collected data in the VCM tree views and list view.

7. "Run Windows Custom Information Reports" on page 114

   Generate your own reports or run existing reports on Windows Custom Information (WCI) data that you collected using your custom PowerShell scripts.

8. "Troubleshooting Custom PowerShell Scripts" on page 115

   If you encounter problems when you run custom PowerShell scripts, run the script as a `.ps1` file and correct any errors before you use the script with a VCM collection filter.

Create Your Own WCI PowerShell Collection Script

Create or modify your Windows Custom Information (WCI) scripts to collect almost any data type that is accessible from VCM managed Windows machines. To return data in a VCM compatible, element-normal XML format, you create your own PowerShell script or obtain PowerShell scripts from VMware Professional Services or another source and modify them for your own collections.

WCI internally stores data in a hierarchy, so your collection script must provide the complete data structure in the standard tree view. The root element in the XML result data set becomes a top-level root element in the WCI data type node. Child elements appear in the same locations in VCM as the locations they populate in the XML document returned by the script.

Prerequisites

- Understand how to write and run PowerShell scripts. See "References on PowerShell and Script Signing" on page 102.
- Plan your data structure to display WCI data in a tree hierarchy based on the data structure specified in the user-defined collection scripts. For an example, see Windows Custom Information Tree View - Standard in the online help.
- Review the guidelines to create PowerShell scripts for WCI collections and understand the challenges. See "Guidelines in PowerShell Scripting for WCI" on page 98.
- Review the example PowerShell script to see a sample script used for a WCI collection. See "Create an Example PowerShell Script for Scheduled Tasks" on page 102.

Procedure

1. On your VCM Collector or managed Windows machine, click **Start**.
2. Select **All Programs > Accessories > Windows PowerShell**.
   - On a 64-bit Windows machine, select **Windows PowerShell (x86)** to run the 32-bit version of PowerShell.
   - On a 32-bit Windows machine, select **Windows PowerShell**.
3. Create your PowerShell script and save it to the location of your choice.

What to do next

Verify that your PowerShell script adheres to valid XML before you can use the script to collect WCI data from VCM managed machines. See "Verify that Your Custom PowerShell Script is Valid" on page 109.

Verify that Your Custom PowerShell Script is Valid

Verify that your PowerShell script adheres to valid XML before you use the script to collect Windows Custom Information (WCI) from VCM managed machines.

To verify that your script is valid, run the script in PowerShell.

Procedure

1. On your VCM Collector or managed Windows machine, open a command prompt.
2. Run `powershell.exe` from the command line.
3. Paste your script into the PowerShell window.

   If your script does not run, press Enter.
4. Make sure that your script runs without errors.

   Errors appear in red in the PowerShell window.
5. If errors occur, resolve them.

   A valid script returns a set of XML content without any formatting, white space, carriage returns, or line feeds at the end of elements, nodes, or attributes.

What to do next

Install PowerShell on your VCM managed machines. See "Install PowerShell" on page 110.

Install PowerShell

Verify that PowerShell 2.0 is installed on each VCM managed Windows machine used to collect Windows Custom Information (WCI).

PowerShell 2.0 is supported on all platforms that support PowerShell 1.0.

- PowerShell is installed by default on Windows 2008 R2 and Windows 7 machines.
- For Windows XP, 2003, 2003 R2, 2008, and Vista machines, you must install PowerShell separately.
- You cannot install PowerShell on Windows 2000 or NT4 machines.

Because of its ability to set the execution policy at the process level, PowerShell 2.0 is the base requirement for WCI in VCM. If you run the standard WCI non-inline collection filters against PowerShell 1.0 VCM managed machines, the collection process will fail.

Procedure

1. On your VCM managed machine, check the following registry entry to verify whether PowerShell 2.0 is installed.
   a. Key Location: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\PowerShellEngine`
   b. Value Name: `PowerShellVersion`
   c. Value Type: `REG_SZ`
   d. Value Data: `<1.0 | 2.0>`

   If you do not check the registry, the steps to determine if PowerShell 2.0 might differ depending on the platform type of your managed machine.

   If PowerShell is not installed on the target VCM managed machine, the WCI collection returns a `Not Executed` status. See "View Windows Custom Information Job Status Details" on page 112.

What to do next

Reboot the VCM managed machine after you install or upgrade PowerShell to ensure that collections work properly.

Collect Windows Custom Information Data

Use the Windows Custom Information (WCI) data type to perform user-defined, script-based collections on your VCM managed machines. To collect the custom data, you build a collection filter that includes a script with parameters to run the script and process the results.

When you use the script-based filter in a collection, the VCM Agent calls a script engine to run the script, parse the results to return the collected data to the VCM database, and display the results in the VCM Console. During the collection process, the VCM Agent starts PowerShell, which runs the script and generates the XML result file. The Agent parses the XML result into a format that VCM can use to check for changes and returns the changes to the Collector.

CAUTION Do not limit collections to deltas when you select a data type in the Collect wizard. If you limit collections to deltas, VCM purges all existing WCI data from the managed machine's master file and from the VCM database, and replaces the WCI data with newly collected data. You must select the option in the Collect wizard so that VCM does not purge WCI data during collections.

Prerequisites

See "Prerequisites to Collect Windows Custom Information" on page 96.

Procedure

1. On your VCM Collector, click **Administration**.
2. Select **Collection Filters > Filters** and click **Add Filter**.
3. On the Name and Description page, type a name and description for the filter and click **Next**.
4. On the Data Type page, select **Windows**.
5. Select the **Custom Information (Win)** data type and click **Next**.
6. On the Windows Custom Information Filter page, select the options to add and configure the filter and click **Next**.

Option	Description
Script Type	Set the format of your PowerShell script to **PowerShell v2.0 Text Output**.
Output Type	Set the resulting output for your PowerShell script to **Element Normal XML**.
Timeout	Retain the default setting of `300` seconds to specify the amount of time the Agent allows a PowerShell script to run before it attempts to end the process. If the script takes more than 300 seconds to run on the VCM managed machine, increase the setting to `900`.
Script	Paste the content of your PowerShell script into the Script text pane. Your script contains statements that are specific to the data type to collect.
Duplicate Handling	Set the method to handle duplicates to **Increment** to resolve duplicate violations of duplicate path attributes in the PowerShell script.

7. On the Important page, review the summary information and click **Finish**.

What to do next

Run a script-based collection filter to collect WCI data using from VCM managed Windows machines. See "Run the Script-Based Collection Filter" on page 111.

Run the Script-Based Collection Filter

Use a collection filter and your PowerShell script to collect Windows Custom Information (WCI) from VCM managed Windows machines.

Procedure

1. On your VCM Collector, click **Collect**.
2. On the Collection Type page, select **Machine Data** and click **OK**.
3. On the Machines page, select the managed machines from which to collect WCI data and click **Next**.
4. Click **Select Data types to collect from these machines** and click **Next**.

   VCM runs a default collection filter for the data type you select.
5. Select **Do not limit collection to deltas** and click **Next**.

   VCM does not purge WCI data during the collection.
6. On the Data Types page, expand **Windows** and select **Custom Information (Windows)**.
7. Click **Select data filters** and click **Next**.
8. On the Filters page, select your WCI filter.
9. Click the arrow to move your filter to the selection area and click **Next**.
10. (Optional) On the Important page, select **View Selected Filter Details** to see details about your collection filter.
11. Click **Close** and click **Finish**.

What to do next

- To confirm that the job finished running, click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.
- View the detailed status about exit codes and standard error output for each job that processed the script or filter. See "View Windows Custom Information Job Status Details" on page 112.

View Windows Custom Information Job Status Details

When you run Windows Custom Information (WCI) collection filter scripts, VCM captures detailed information and displays status about exit codes and standard error output for each job that processed the script or filter. You can view the job status details in Job Manager.

The following procedure displays data for an instant collection performed in the last 24 hours.

Prerequisites

- Verify that all prerequisite components exist on the VCM managed machine. If a prerequisite component such as PowerShell is not installed or available on the managed machine, the script cannot run and a status of `Not Executed` appears in the Status column. Because optional components such as PowerShell or other script engines might not be supported for installation on all VCM-supported OS versions, a `Not Executed` status does not result in a failure.
- Collect Windows Custom Information. See "Collect Windows Custom Information Data" on page 110.

Procedure

1. On your VCM Collector, click **Administration**.
2. Select **Job Manager > History > Instant Collections > Past 24 Hours**.
3. In the Instant Collections pane, select a collection job that includes WCI data.
4. In the Job History Machine Detail pane, select **View Details**.

   A single row appears for each WCI filter that ran in the collection job. Information about the WCI script and the script results parsing appears in the row.
5. In the View Details by Machine window, select the managed machines to view and click **OK**.

   Detailed job history results appear for the WCI filters and managed machines.

   - If a WCI collection job encounters errors on a VCM managed machine, VCM reports detailed information about the failure. Failures can occur when PowerShell starts, during script execution, or when interpreting the script results.
   - If PowerShell is not installed on the managed machine, an error can occur in the PowerShell startup process. Because PowerShell is an optional component, a status of `Not Executed` can appear in the job details to indicate the skipped steps. The `Not Executed`status does not appear as an error in the VCM job.
   - If a PowerShell script generates errors due to defects in the script, such as syntactical or typographical errors, VCM reports the status as finished with errors in the collection job.

What to do next

- Review the WCI collection results. See "Windows Custom Information Collection Results" on page 113.
- Generate your own reports. See "Run Windows Custom Information Reports" on page 114.

Windows Custom Information Collection Results

Examine the results of your Windows Custom Information (WCI) collected data in the VCM tree views and list view.

Prerequisites

Collect WCI data and confirm that the WCI collection job finished. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**. See "Collect Windows Custom Information Data" on page 110.

Procedure

1. On your Collector, click **Console**.
2. Select **Windows > Operating System > Custom Information**.
3. Select a view of the collected WCI data.

Option	Description
Tree View - Standard	Tree hierarchy view based on the data structure in your PowerShell script.
Tree View - Consolidated	Tree hierarchy that displays data across multiple elements simultaneously with the data consolidated from one level of the tree. The child node properties and values appear in each node.
List View	Data organized by a list of top-level elements. You can filter, sort, or group the data.

What to do next

Generate your own reports. See "Run Windows Custom Information Reports" on page 114.

Run Windows Custom Information Reports

Generate your own reports or run existing reports on Windows Custom Information (WCI) data that you collected using your custom PowerShell scripts.

Prerequisites

Collect WCI data. See "Collect Windows Custom Information Data" on page 110.

Procedure

1. On your VCM Collector, click **Reports**.
2. Select **Machine Group Reports > Windows > Custom Information**.
3. Select a custom information report.

Option	Description
Netstat Open Ports Information	Reports port and protocol information from the `netstat -A` command.
SQL SMO Database Information	Reports the database details collected.
SQL SMO Instance Information	Reports basic information about the SQL Server instances collected.

4. Click **Run**.

   The report displays information about the collected WCI data. For example, the NetStat Open Ports Information report displays the protocol, port, remote port, local address, foreign address, port state, and the collection filter used in the collection.

Troubleshooting Custom PowerShell Scripts

If you encounter problems when you run custom PowerShell scripts, run the script as a `.ps1` file and correct any errors before you use the script with a VCM collection filter.

Prerequisites

- Verify that your script runs in PowerShell. See "Verify that Your Custom PowerShell Script is Valid" on page 109.
- Understand the PowerShell script signing policies. See "PowerShell Script Signing Policies" on page 101.

Procedure

1. On your VCM Collector, save the script to a file that has the `.ps1` extension.
2. Run the script file from a command line using PowerShell 2.0 or PowerShell 1.0.
   - For PowerShell 2.0, run:
     ```
     PowerShell –command set-executionpolicy RemoteSigned –scope Process ;
     scriptname.ps1 > resultfile.xml
     ```
   - For PowerShell 1.0, set the execution policy to Remote Signed or use a less restrictive policy, and run:
     ```
     PowerShell –file scriptname.ps1 > resultfile.xml
     ```

   When the script is finished running, it generates the XML file.
3. Verify that you can open the XML file in Internet Explorer.
   - If you cannot see the entire file, allow blocked content.
   - If Internet Explorer cannot parse the XML file, you must correct any formatting errors.

   If you have Visual Studio installed, you can use it locate formatting errors in large XML files.

What to do next

- Re-run your custom PowerShell script to verify that it runs correctly. See "Collect Windows Custom Information Data" on page 110.
- View the detailed status about exit codes and standard error output for each job that processed the script or filter. See "View Windows Custom Information Job Status Details" on page 112.
- After the Windows Custom Information data is available in the VCM database, you can generate reports and enforce compliance. See the online help.

Configuring Linux, UNIX, and Mac OS X Machines

8

To manage machines running Linux, UNIX, and Mac OS X operating systems, you must license the machines, install the VCM Agent on the machines, and begin collecting data.

The Agent manages the communication between the VCM Collector and the Linux, UNIX, and Mac OS X machines. You can use VCM to install the Agent on the target machines, or you can install the Agent using a manual process. For the manual Agent installation process, see the online Help.

This chapter includes the following topics:

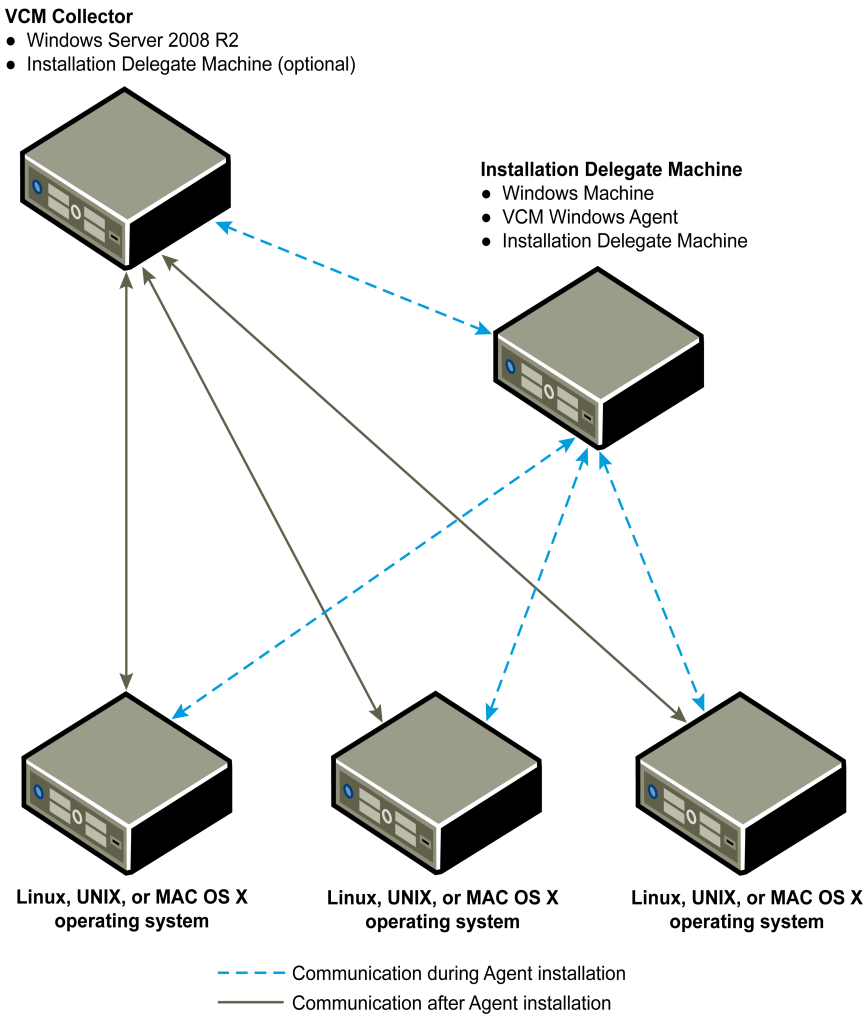
Configure Collections from Linux, UNIX, and Mac OS X Machines 120
Linux, UNIX, and Mac OS X Collection Results 133
Configure Scheduled Linux, UNIX, and Mac OS X Collections 133

Linux, UNIX, and Mac OS X Machine Management

VCM manages your Linux, UNIX, and Mac OS X machines using the VCM Agent. The Agent manages communication between the Collector and the Linux, UNIX, and Mac OS X machines, including collecting data and running actions. Compliance and change are monitored based on the collected data.

To install the Agent on the target machines, you first configure one or more Installation Delegate machines. An Installation Delegate is a Windows machine that is running one of the supported operating systems and on which the VCM Windows Agent is installed. It is the machine that manages communication between the Collector and the target machines during the Agent installation process. It is also the machine that pushes the correct Agent files to target machines. After the Agent is installed, the Installation Delegate no longer has a role in the management of Linux, UNIX, and Mac OS X machines. The Agent handles communication between the Collector and the managed machine.

Figure 8–1. Linux, UNIX, and Mac OS X Managed Machines Diagram


VCM Collector
• Windows Server 2008 R2
• Installation Delegate Machine (optional)
Installation Delegate Machine
• Windows Machine
• VCM Windows Agent
• Installation Delegate Machine
Linux, UNIX, or MAC OS X operating system
Linux, UNIX, or MAC OS X operating system
Linux, UNIX, or MAC OS X operating system
Communication during Agent installation
Communication after Agent installation

Installation Delegates for Linux, UNIX, and Mac OS X Agent Installations

The Installation Delegate machines run a supported Windows operating system and must have the 5.5 Agent or later installed. They must also be configured to manage the secure communication between the target Linux, UNIX, or Mac OS X machines and the Collector. Depending on the number of machines on which you are installing the Agent with one action, you can use your Collector as a Installation Delegate, or you can use another Windows machine.

If the target Linux, UNIX, or Mac OS X machines are located on a site remote from your Collector where the network bandwidth from the Collector to the target machines is not sufficient to support the installation process, you can configure a Installation Delegate at the target site. The Installation Delegate will help to load balance the installation of the Agent files to the target machines by first downloading a copy of the requested Agent files, and then pushing the files to the target machines for installation.

Managing Linux, UNIX, and Mac OS X Machines

Using the VCM Agent, which is installed on the Linux, UNIX, and Mac OS X machines, you collect configuration data from the machines. You can then run compliance against the collected data, monitor the machines for change, and perform selected actions, such as changing property values.

Linux, UNIX, or Mac OS X Installation Credentials

The installation credentials required to install the VCM Agent on Linux, UNIX, or Mac OS X machines must have sufficient privileges to copy the Agent files to the target machines and run the installation process. You have several options for providing the credentials, including during installation process at a job or object level, or configuring the credentials as administrative parameters.

You must provide the User Name, Password, and Root Password for your credentials. Even when the User Name is root, you must provide the root password as both the Password and as the Root Password. The installation process uses SSH and SCP to connect from the Installation Delegate machine to the target machine. The credentials used for these connections are those specified as User Name and Password. Once the files have been copied over, the installation process calls su to elevate to root access so it can install the VCM agent. The password used for su is the one specified as Root Password.

Installation Wizard Credentials

You can provide the installation process credentials in the installation wizard when you install the Agent. The credentials, which are the user name, password, and root password, can be configured at the object or job level. The object level option requires you to provide the credentials separately for each machine. The job level allows you to use the same credentials for a single installation action on one or more machines.

You will find these options in **Administration > Machines Manager > Licensed Machines > Licensed UNIX Machines > UNIX/Linux Agent Install** wizard.

Administrative Parameter Credentials

You can define installation credentials as administrative parameters that are used to install the Agent when object or job level credentials are not provided in the installation wizard. The UNIX/Linux Agent Install parameters allow you to define the context, which determines at what level the provided credentials are applied. The levels, from the most specific to the most general, are Machine, Machine Group, Domain, and SRF Action Script Global.

For example, if you have machines, A, B, C, and so on, where A through C belong to the Dev machine group and the rest are not part of the Dev machine group, and you add a Machine context parameter and a Machine Group context parameter, then the processing order determines the level at which the user name and password are processed.

If machines A and B are configured with the name and password at the machine level, then the Machine parameter is used, even though they belong to the same machine group as machine C.

If machine C is configured with the user name and password at the machine group level, then the Machine Group parameter is used.

If machines D, and so on, are machines that are not configured with machine, machine group, or domain level user names and passwords in the SRF Administrative Parameters and are configured with SRF Action Script Global, then the SRF Action Script Global parameter is used.

You will find these options in **Administration > Settings > Scripted Remediation Framework > Administrative Parameters > Add or Edit** wizard.

Processing the Credentials During Installation

During the installation process, the installation wizard will first process the credentials in the following order:

1. Installation wizard Object level credentials
2. Installation wizard Job level credentials
3. Administrative parameter Machine context credentials
4. Administrative parameter Machine Group context credentials
5. Administrative parameter Domain context credentials
6. Administrative parameter SRF Action Script Global context credentials

Credential Processing Scenarios

The following scenarios further demonstrates how the credentials are processed.

- You do not provide object or job level credentials, nor did you configure any administrative parameters.

  The installation job fails due to lack of credentials.

- You provide object or job level credentials, but you did not configure any administrative parameters.

  The installation job runs using the credentials you provided in the installation wizard.

- You do not provide object or job level credentials, but you already configured administrative parameters for one or more of the credential contexts, which are Machine, Machine Group, Domain, or SRF Action Script Global.

  The installation job runs using the credentials configured in the administrative parameters.

- You provide user name and password credentials that have root privileges, in the installation wizard or in the administrative parameters, but you do not provide the root password.

  The installation fails due to insufficient privileges.

Configure Collections from Linux, UNIX, and Mac OS X Machines

To collect Linux, UNIX, and Mac OS X data from your virtual or physical machines, you must install the VCM Agent. To install the Agent, you must configure an Installation Delegate, either the Collector or another Windows machine, add the target machines, license them for use, and install the VCM Agent.

Procedure

1. "Configure Installation Delegate Machines to Install Linux, UNIX, and Mac OS X Agents" on page 121

   The Installation Delegate machines are one or more virtual or physical machines that manage the communication between the Collector and your target Linux, UNIX, or Mac OS X machines during the VCM Agent installation process.

2. "Configure the HTTPS Bypass Setting for Linux Agent Installations" on page 123

   If your Collector is not configured to use HTTPS, you must configure the Collector to allow HTTP communication when entering sensitive parameter values.

3. "Enable Linux, UNIX, and Mac OS X Agent Installation" on page 123

   You configure the Enable Automated Linux Agent Install option so that you can use VCM to install the Agent on Linux, UNIX, and Mac OS X machines.

4. "Add and License Linux, UNIX, and Mac OS X Machines for Agent Installation" on page 124

   You must add and license Linux, UNIX, and Mac OS X machines so that you can install the Agent manage them in VCM.

5. "Install the VCM Agent on Linux, UNIX, and Mac OS X Operating Systems" on page 125

   To enable communication between the Collector and the managed machines, install the VCM Agent on Linux, UNIX, or Mac OS X machines.

6. "Collect Linux, UNIX, and Mac OS X Data" on page 132

   To begin managing the machine on which you installed the VCM Agent, you must perform an initial collection, which adds the data to VCM.

Configure Installation Delegate Machines to Install Linux, UNIX, and Mac OS X Agents

The Installation Delegate machines are one or more virtual or physical machines that manage the communication between the Collector and your target Linux, UNIX, or Mac OS X machines during the VCM Agent installation process. After the Agent is installed, the Installation Delegate is not required to collect data or manage the target Linux, UNIX, or Mac OS X machines.

The Installation Delegate machines run a supported Windows operating system and must have the 5.5 Agent or later installed. They must also be configured to manage the secure communication between the target Linux, UNIX, or Mac OS X machines and the Collector. Depending on the number of machines on which you are installing the Agent with one action, you can use your Collector as a Installation Delegate, or you can use another Windows machine.

If the target Linux, UNIX, or Mac OS X machines are located on a site remote from your Collector where the network bandwidth from the Collector to the target machines is not sufficient to support the installation process, you can configure a Installation Delegate at the target site. The Installation Delegate will help to load balance the installation of the Agent files to the target machines by first downloading a copy of the requested Agent files, and then pushing the files to the target machines for installation.

Prerequisites

Verify that the machines that you are configuring as the Installation Delegates are running Windows Server 2008 R2 and Windows 7, 64-bit.

Procedure

1. "Collect Machines Data From Linux Agent Installation Delegate Machines" on page 121

   You collect data from your Installation Delegate machines to ensure that VCM identifies the Windows machines as licensed and that the 5.5 Agent or later is installed.

2. "Set the Trust Status for Linux Agent Installation Delegate Machines" on page 122

   You can set the trusted status on machines where you have verified that the connection is legitimate. When you set the trust status, you are marking the Agent certificate as trusted.

3. "Enable Installation Delegate Machines for Linux Agent Installation" on page 123

   Installation Delegate machines must be enabled to perform the necessary communication between the VCM Collector and your target Linux, UNIX, and Mac OS X machines.

Collect Machines Data From Linux Agent Installation Delegate Machines

You collect data from your Installation Delegate machines to ensure that VCM identifies the Windows machines as licensed and that the 5.5 Agent or later is installed.

The Installation Delegate is used to manage the communication between the Collector and the target Linux or UNIX machines during the Agent installation process.

Prerequisites

Verify that the Installation Delegate machine is licensed and that it has the VCM Agent 5.5 or later installed. See "Configure Windows Machines" on page 87.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed Windows Machines**.
3. Select the target machines and click **Collect** on the VCM toolbar.
4. Select **Machine Data** and click **OK**.
5. Verify that the Selected list includes the target machines and click **Next**.
6. Expand the **Windows** tree, select **Machines**, and click **Next**.
7. Resolve any conflicts and click **Finish**.

What to do next

- When the job is finished, verify that the Agent Version value in the Licensed Windows Machines data grid is 5.5 or later.
- Configure the trust status for the Installation Delegates. See "Set the Trust Status for Linux Agent Installation Delegate Machines" on page 122.

Set the Trust Status for Linux Agent Installation Delegate Machines

You can set the trusted status on machines where you have verified that the connection is legitimate. When you set the trust status, you are marking the Agent certificate as trusted.

When you transmit sensitive information, such as credentials, between the Collector and virtual or physical machines configured as your Installation Delegate, the Agent certificate, including the Agent certificate on the Collector, must be trusted.

If you do not use this level of security, you can set the `Allow sensitive parameters to be passed to agents not verified as Trusted` option to `Yes`. The override setting is located in the **Collector General Settings** in **Administration**.

Prerequisites

Collect the Machines data type from the Windows machines you are using as Installation Delegates. See "Collect Machines Data From Linux Agent Installation Delegate Machines" on page 121.

Procedure

1. Click **Administration**.
2. Select **Certificates**.
3. Select the target machines and click **Change Trust Status**.
4. Add any additional machines to trust to the lower data grid.
5. Select **Check to trust or uncheck to untrust the selected machines** and click **Next**.
6. Review the number of machines affected and click **Finish**.

What to do next

Identify the Windows machines as Installation Delegates. See "Enable Installation Delegate Machines for Linux Agent Installation" on page 123.

Enable Installation Delegate Machines for Linux Agent Installation

Installation Delegate machines must be enabled to perform the necessary communication between the VCM Collector and your target Linux, UNIX, and Mac OS X machines.

Prerequisites

Ensure that the Installation Delegate machines are trusted machines. See "Set the Trust Status for Linux Agent Installation Delegate Machines" on page 122.

Procedure

1. Click **Administration**.
2. Select **Administration > Certificates**.
3. Select the target machines and click **Installation Delegate**.
4. Add any additional machines to the lower data grid.
5. Select **Enable - allow the selected machines to be used as an installation delegate** and click **Next**.
6. Review the number of machines affected and click **Finish**.

What to do next

If your Collector is not configured to use HTTPS, set the HTTPS bypass. See "Configure the HTTPS Bypass Setting for Linux Agent Installations" on page 123.

Configure the HTTPS Bypass Setting for Linux Agent Installations

If your Collector is not configured to use HTTPS, you must configure the Collector to allow HTTP communication when entering sensitive parameter values.

If your Collector is configured to use HTTPS, you do not need to modify this setting.

Procedure

1. Click **Administration**.
2. Select **Settings > General Settings > Collector**.
3. Select **Allow HTTP communication (HTTPS bypass) when entering sensitive parameter values** and click **Edit Settings**.
4. Select **Yes** and click **Next**.
5. Review the summary and click **Finish**.

What to do next

Enable Linux, UNIX, and Mac OS X Agent installations. See "Enable Linux, UNIX, and Mac OS X Agent Installation" on page 123.

Enable Linux, UNIX, and Mac OS X Agent Installation

You configure the Enable Automated Linux Agent Install option so that you can use VCM to install the Agent on Linux, UNIX, and Mac OS X machines.

When you use VCM to install the Agent, the installation process uses SSH to copy the Agent files from the Installation Delegate machine to the target machines using ordinary user credentials, and then installs the Agent as root user. Sensitive administration passwords are stored using the Local Data Protection Service API. However, since the process does not validate the device thumbprint before installing the Agent, you should not use this process unless you are certain that your network is secure and impervious to machine impersonation.

Procedure

1. Click **Administration**.
2. Select **Settings > General Settings > Collector**.
3. Select **Enable Automated Linux Agent Install** and click **Edit Setting**.
4. Select **Yes** and click **Next**.
5. Verify the change and click **Finish**.

What to do next

Add Linux, UNIX, or Mac OS X machines to VCM. See "Add and License Linux, UNIX, and Mac OS X Machines for Agent Installation" on page 124.

Add and License Linux, UNIX, and Mac OS X Machines for Agent Installation

You must add and license Linux, UNIX, and Mac OS X machines so that you can install the Agent manage them in VCM.

If you are adding a large number of machines, there are several methods that you can use, including importing machine information from a file, IP discovery, DB discovery, or Nmap discovered machines.

NOTE You can use the Discovered Machines Import Tool (DMIT), which imports machines discovered by the Network Mapper (Nmap), to import many physical and virtual machines at one time into the VCM database. Download DMIT from the VMware Web site.

This procedure uses the manual process to add the machines to VCM and to license them when they are added. However, you can use one of the other methods. See the Discovery Rules in the online Help if you want to use another method to add machines.

Prerequisites

Verify that you know the name or IP address, domain, domain type, machine type, and the communication port for the machines you are adding to VCM.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed UNIX Machines**.
3. Click **Add Machines**.
4. Select **Basic**, select **Automatically license machines**, and click **Next**.
5. Add the Linux, UNIX, or Mac OS X machines to the list.

a. Configure machine information.

Option	Action
Machine	Type the name of the machine. You can use NetBIOS or Fully-Qualified Domain Name (FQDN) notation for the name. If your Collector cannot resolve a host name with a DNS Server, use an IP address rather than a machine name.
Domain	Type or select the domain to which the machine belongs.
Type	Select the domain type.
Machine Type	Select the machine type. You must select the correct machine type to ensure that the machine is correctly managed in VCM.
Port	Type the port number. The default value is 26542 when you select a Linux, UNIX, or Mac OS X machine type. The port number must be the same number used when you install the Agent on the managed machine.

b. Click **Add**.

c. To add other machines, configure the machine information and click **Add**.

d. After you add the target machines, click **Next**.

6. Review the machine information and click **Finish**.

   The machine is added to the Licensed UNIX Machines data grid.

What to do next

Install the VCM Agent on target machines. See "Install the VCM Agent on Linux, UNIX, and Mac OS X Operating Systems" on page 125.

Install the VCM Agent on Linux, UNIX, and Mac OS X Operating Systems

To enable communication between the Collector and the managed machines, install the VCM Agent on Linux, UNIX, or Mac OS X machines.

When you start an installation action for Linux, UNIX, or Mac OS X machines, the Agent files for the target operating systems are downloaded to the Installation Delegate machine and the Installation Delegate then copies the appropriate operating system Agent files to each of your target machines. After the files are copied to the target machines, the files are unpacked and the Agent is installed with the options you specified when you configured the installation action.

On the Collector, the Agent files are located in `\VMware\VCM\Installer\Packages`.

If you use the Collector as your managing Agent, the Agent files are copied to `\VMware\VCM\Installer\Content\CMAgent.{version}.{Linux, Solaris, AIX, HP-UX, or Darwin (Mac OS X)}`.

If you use another Windows machine as an Installation Delegate, the Agent files are copied to`\WINDOWS\CMAgent\CMAgent{Linux, Solaris, AIX, HPUX, or Darwin}`.

This procedure uses VCM to install the Agent on your target machines. You might also use a manual process. See the online Help for the steps to manually install the Agent on your Linux, UNIX, and Mac OS X machines.

Prerequisites

- If you are not using the Collector as your Installation Delegate machine, configure a managed Windows machine as your Installation Delegate. See "Configure Installation Delegate Machines to Install Linux, UNIX, and Mac OS X Agents" on page 121.
- If your Collector is not configured to use HTTPS, you must configure the Collector to allow HTTP communication when entering sensitive parameter values. See "Configure the HTTPS Bypass Setting for Linux Agent Installations" on page 123.
- Enable VCM to allow Linux Agent installations. See "Enable Linux, UNIX, and Mac OS X Agent Installation" on page 123.
- Ensure that the target machines appear in the Licensed UNIX Machines data grid. See "Add and License Linux, UNIX, and Mac OS X Machines for Agent Installation" on page 124.
- Verify that the machine on which you intend to install the Agent has enough free disk space. For more information, see the *VCM Installation Guide*.
- Verify that you know the user name and password for the target machines. The credentials must have sufficient permissions to copy the Agent files to the machine and run the installation process. See "Linux, UNIX, or Mac OS X Installation Credentials" on page 119.
- Verify that the SSH service is running on the target machines and that the user who is installing the Agent can connect to the machines through the SSH service.
- If your target machines are 64-bit, you must install the 32-bit version of the GNU C library (glibc) on your 64-bit target machines.
- Disable or reconfigure firewalls on the target machines to allow Agent installation. The default port for Agent communication with VCM is 26542. You can add this port to your exceptions list in your firewall rule.
- If you are collecting non-ASCII information from the target machines, install a UTF-8 locale. To determine the locales installed on your operating system, use the `locale -a` command.
- Review the Agent installation parameters to ensure that you understand the optional settings that appear in the wizard. See "Agent Installation Parameters for Linux, UNIX, or Mac OS X Machines" on page 127.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed UNIX Machines**.
3. Select one or more target machines and click **Install**.
4. Add or remove target machines from the lower list and click **Next**.
5. If you must change a default parameter value, add one or more optional parameters to the lower list and click **Next**.

   The options, which are configured on the following wizard pages, apply to all the selected target machines.

If you select User Name, Password, and Root Password at the object level, you configure each target machine individually. If you select the options at the job level, you configure the options for all the target machines for this installation action.

The default Thread Pool Size is 10. This option determines how many Agent installations can run in parallel during one installation actions. Depending on the CPU and RAM of the Managing Agent machine, you might need to change this value.

6. Configure the installation options and click **Next**.
   a. Select the Installation Delegate machine for this installation action.

      When you click the ellipsis button, only the Windows machines that are configured as Installation Delegates appear in the list.

   b. If you are upgrading to the latest Agent, select **Yes**.

      The old Agent is uninstalled before the latest Agent is installed.

   c. Configure the selected installation parameters.
7. If you selected User Name, Password, or Root Password, configure the values for your target machines and click **Next**.

   You must provide the User Name, Password, and Root Password for your credentials. Even when the User Name is root, you must provide the root password as both the Password and as the Root Password. The installation process uses SSH and SCP to connect from the Installation Delegate machine to the target machine. The credentials used for these connections are those specified as User Name and Password. Once the files have been copied over, the installation process calls su to elevate to root access so it can install the VCM agent. The password used for su is the one specified as Root Password.
8. To install the VCM Agent immediately, select **Run action now** and click **Next**.
9. Review the number of target machines and click **Finish**.

The Agent is installed at the specified time on the target machines.

What to do next

- Verify that the jobs finished running. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.
- Collect data from the managed Linux, UNIX, or Mac OS X machines. See "Collect Linux, UNIX, and Mac OS X Data" on page 132.

Agent Installation Parameters for Linux, UNIX, or Mac OS X Machines

The installation parameters are variables that you modify as needed when you install the VCM Agent on Linux, UNIX, or Mac OS X target machines.

Installation Options with Default Values	Description
`CSI_AGENT_RUN_OPTION`	You can install the Agent as a daemon process or installed to be run by `inetd/xinetd/launchd`. ■ A value of inetd installs the Agent for execution by `inetd/xinetd/launchd`. ■ A value of daemon installs the agent for execution as a daemon process.

Installation Options with Default Values	Description
CSI_BIND_IP	Binds the Agent to a single IP address. This value is only honored in daemon mode.
CSI_NO_LOGIN_SHELL= +S:+A :+/sbin/noshell+/bin/false+ /sbin/false+/usr/bin/false +/sbin/nologin CSI_NO_LOGIN_SHELL= +D :+/sbin/noshell+/bin/false+ /sbin/false+/usr/bin/false +/sbin/nologin	The CSI_USER account must not have a login shell. This parameter lists all valid no-login shells and is used to verify the CSI_USER has no-login shell. If your system has a valid no login shell that is not listed, you append a plus sign and add the no login shell to the list. The options available for this parameter include: ■ +S means only for Solaris ■ +A means only for AIX ■ +H means only for HP-UX ■ +L means only for Linux ■ +D means only for Darwin (Mac OS X) ■ + means for all operating systems
CSI_CREATE_USER=Y	Keep the default value. Indicates whether the user will be created. When you install in trusted mode on HP-UX v1.0 (11.11), the user must exist on the target machine. If you attempt to install and create the user, the installation of the Agent fails.
CSI_ROOT_NAME	Name of the directory where the Agent files are located. The default value is CMAgent.
CSI_USER_ID=501	Keep the default value. Integer value for the user ID of the created user.
CSI_USER_NO_LOGIN_ SHELL=/bin/false	Keep the default value. Indicates the no-login shell value to use when you create the user.
CSI_USER_PRIMARY_GROUP=csi_ acct	Keep the default value. Group name to use when you create a new user as the user's primary group. This group is for low security access. Most inspections are executed with the lowest possible privileges using this group while also preventing access by way of this group to the high security group privileges.
CSI_CREATE_USER_PRIMARY_ GROUP=Y	Keep the default value. Indicates the need to create a low-security primary group for the CSI_USER.
CSI_USER_PRIMARY_GID=501	Keep the default value. Create user's primary Group ID.
CSI_USER_USE_NEXT_ AVAILABLE_LOCAL_GID=Y	Keep the default value. Setting this option to Y allows the Group ID to be the next available local Group ID over CSI_ USER_PRIMARY_GID.

Installation Options with Default Values	Description
CSI_USER=csi_acct	Keep the default value. The user assigned to the cfgsoft group. The CSI listener process runs under this user.
CSI_CFGSOFT_GID=500	Keep the default value. The Group ID of the cfgsoft group. This value can change if the GID is already in use. This group is for high-security access. Some inspections require root privileges, which are provided indirectly through this group and setuid to root.
CSI_CREATE_LOCAL_GROUP=Y	Keep the default value. Setting this option to Y allows the cfgsoftgroup to be created. This setting allows the system call to groupadd.
CSI_USE_NEXT_AVAILABLE_ LOCAL_GID=Y	Keep the default value. Setting this option to Y allows this Group ID to be the next available local Group ID starting at CSI_CFGSOFT_GID.
CSI_AGENT_PORT=26542	Keep the default value. Specifies the port on which the Agent listens.
CSI_CREATE_LOCAL_SERVICE=Y	Keep the default value. Setting CSI_CREATE_LOCAL_ SERVICE to Yallows the system to create the local service (copy files to system directories).
CSI_REFRESH_INETD=Y	Setting this option to Y allows the system to refresh xinetd (Linux) or inetd (Solaris, AIX, and HP-UX). Keep default value only if you are running your agent as inetd. If you are running your agent as a daemon, select CSI_REFRESH_ INETD=N This option does not apply to Mac OS X.
CSI_NICE=10	Keep the default value. Sets the nice value for the agent listener process.
CSI_CERTIFICATE_PATH=	Specifies the path to Collector Certificates. The certificates specified at this path are copied to the Agent. If your Collector Certificates are stored in an accessible location on this machine, you use this option to put the certificates in the Agent location. You should install the Enterprise Certificates so that multiple collector instances collecting from the same set of Agents is supported. If this package was copied from a collector installation, this package already contains that Collector's Enterprise Certificate.
CSI_PARENT_DIRECTORY=/opt	Specifies the parent directory of the CM Agent. The root directory of CMAgent will be CSI_PARENT_ DIRECTORY/CMAgent.
CSI_PARENT_DATA_ DIRECTORY=/opt	Specifies the parent directory of the CMAgent data directory. The data directory will be CSI_PARENT_DATA_DIRECTORY/ CMAgent/data.

Installation Options with Default Values	Description
CSI_PARENT_LOG_ DIRECTORY=default	Specifies where agent operational log files are kept. The log directory is CSI_PARENT_LOG_DIRECTORY/CMAgent/log. The default value indicates to use these values. ■ Linux: /var/log ■ AIX, HP-UX, and Solaris: /var/adm ■ Mac OS X: log ->private/var/log/CMAgent/log
CSI_KEEP_CSIINSTALL=N	Recommend keeping the default value. After a successful installation, the temp installation directory CSIInstall is deleted. To keep this installation directory, set this parameter to Y.

Installation Options with Default Values	Description
CSI_LOCALE=	Keep the locale configuration option unspecified in the csi.config file when installing the Agent. If you configure the value, it supercedes the data encoding locale on the target operating system. The locale, which should be a UTF-8 locale, affects the internal data conversions on non-ASCII data performed by VCM, but the setting does not affect how the collected data is displayed in VCM. This configuration value is used to resolve any problems with data conversions after you install the Agent. If this value is left blank, the Agent installation scripts attempt to find an appropriate value for the CSIRegistry base on the following rules presented in order of precedence. 1. The optional CSI_LOCALE value set is in the csi.config file. By default, the entry is blank in the csi.config file package in the Agent. If this value is set, the Agent installation script uses the provided value. During the installation of the Agent, the value is checked against the operating system to ensure that it is a valid value. If the value is not valid, it is still used and is set as the value in the CSIRegistry, but the process logs and displays an installation error. The Agent uses what is in the CSIRegistry. 2. The default locale on the target operating system at installation time is {some locale value}.utf8. For example, en_US.UTF-8. The value is added to the CSIRegistry. 3. The default locale on the target operating system is not UTF-8, but has a UTF-8 locale installed. For example, if the default locale is en_US.8859-15 and en_US.UTF-8 is installed on the system, en_US.UTF-8 is used. The UTF-8 locale is added to the CSIRegistry. 4. No default locales are specified on the target operating system. The Agent installation script runs the locale -a command and adds the first installed UTF-8 locale that it finds to the CSIRegistry. 5. The operating system is not configured for any internationalization. The C locale, which is the locale that is used to specify plain ASCII, is added to the CSIRegistry, but processes the logs and displays an i18n warning. If you interactively install the Agent, the Agent installation

Installation Options with Default Values	Description
	scripts use the previous precedence rules to evaluate and generate a default value that is displayed during the installation of the Agent. If you select a non-UTF-8 locale, the Agent installation uses the locale, but the process logs and displays a warning. If you select a locale that does not exist on the operating system, the Agent installation uses the locale, but the process logs and displays an error.

Collect Linux, UNIX, and Mac OS X Data

To begin managing the machine on which you installed the VCM Agent, you must perform an initial collection, which adds the data to VCM.

Use the default filter set to collect data that provides a general view of the Linux, UNIX, and Mac OS X machines in your environment. The first time you use the default filter to collect data, the Agent collects all the data specified in the filter and stores the data in the VCM database. All subsequent collections return a delta based on the previously collected data unless you override the option and collect all the data.

Prerequisites

- Verify that the Linux, UNIX, and Mac OS X machines are licensed. See "Add and License Linux, UNIX, and Mac OS X Machines for Agent Installation" on page 124.
- Ensure that the Agent is installed on the target machines. See "Install the VCM Agent on Linux, UNIX, and Mac OS X Operating Systems" on page 125.

Procedure

1. Click **Collect**.
2. On the Collection Type page, select **Machine Data** and click **OK**.
3. On the Machines page, select the machines from which you are collecting data and click **Next**.
4. On the Data Types page, configure the collection and click **Next**.
   a. Expand Unix and select the data types.

      At a minimum, you must collect **Machines - General** data. If you are managing data using compliance, change, or running reports, you must collect the data types that are included in the other actions or that you want to view in the appropriate data grids.

   b. Select **Use default filters**.
5. On the Important page, verify that there are no conflicts with previously scheduled or running jobs, and click **Finish**.

   The amount of time the first collection requires is determined by the number of machines and network connectivity.
6. Click **Administration** and select **Job Manager > History > Instant Collections > Past 24 Hours** to determine if the collection finished.

   The amount of time the collection requires is determined by the number of machines and network connectivity.

What to do next

- Review the collected data from the managed machines. See "Linux, UNIX, and Mac OS X Collection Results" on page 133.
- (Optional) Schedule regular data collections from managed machines. See "Configure Scheduled Linux, UNIX, and Mac OS X Collections" on page 133.

Linux, UNIX, and Mac OS X Collection Results

Collected Linux, UNIX, and Mac OS X data appears in the VCM data grids and is available for several management actions.

The displayed data is only as current as the last time you collected data.

Option	Description
Console	Displays dashboards and summary reports based on collected data. You use the Console to view data relevant to day-to-day operations, troubleshooting, and analysis. To view the dashboards, click **Console** and select **Dashboards > UNIX**. To view the summary reports, click **Console** and select **UNIX tab > Operating System > Machines > General**. You can view the data in a summary report or data grid format.
Compliance	Determines if the collected data from target machines meets specified compliance values, and allows you to run compliance remediation actions. To run a compliance check, click **Compliance** and select **Machine Group Compliance** and follow the steps described in the online help to create rule groups, rules, filters, and templates.
Reports	Runs preconfigured VCM reports or you can create custom reports. Reports are run against currently collected data. Depending on the volume or complexity of the data requested in a report, it may take time to generate the report. See UNIX Reports in the online Help for information about scheduling and disseminating reports. To use the reporting options, click **Reports** and select **Machine Group Reports > UNIX**.
Patching	Assesses target machines to determine if the machines have the most current patches. If the patches are not yet installed, you can install the latest patches on the target machines. To assess and patch machines, select **Patching**, and select your target operating system.

What to do next

- (Optional) To ensure data is collected regularly, schedule collections. See "Configure Scheduled Linux, UNIX, and Mac OS X Collections" on page 133.

Configure Scheduled Linux, UNIX, and Mac OS X Collections

You can configure VCM to regularly collect Linux, UNIX, and Mac OS X data from machine groups to ensure that you are using current results when you are viewing the data and when you run reports or compliance.

This action is not required, but scheduling your collections improves your configuration management efficiency.

Prerequisites

Verify that your Linux, UNIX, and Mac OS X machines are managed machines. See "Configure Collections from Linux, UNIX, and Mac OS X Machines" on page 120.

Procedure

1. "Create a Dynamic Machine Group for Linux, UNIX, or Mac OS X Machines" on page 134

   To schedule collections from particular Linux, UNIX, or Mac OS X machines, you must create machine groups that include the machines from which you want to collect information and that you want to manage as a group.

2. "Schedule Linux, UNIX, and Mac OS X Collections" on page 135

   Scheduled collection jobs run against your Linux, UNIX, and Mac OS X machine group to regularly collect data from the managed machines.

Create a Dynamic Machine Group for Linux, UNIX, or Mac OS X Machines

To schedule collections from particular Linux, UNIX, or Mac OS X machines, you must create machine groups that include the machines from which you want to collect information and that you want to manage as a group.

The machine groups can include many machine types, not just Linux, UNIX, or Mac OS X.

In this procedure, you create a dynamic machine group for Red Hat and SUSE machines. As new machines are added to VCM that meet the filter criteria, the machines are included in the machine group.

Prerequisites

Ensure that you collected data from the machines you are including in the group. See "Collect Linux, UNIX, and Mac OS X Data" on page 132.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Machine/Virtual Object Groups > All Machines > All UNIX Machines**.
3. Click **Add Group**.
4. Type the name and description of the machine group and click **Next**.

   For example, type the name Dynamic Linux Group.

5. Select **Dynamic** and click **Next**.
6. Click **Finish**.

   The group is added to the All Machines list.

7. Expand your group in the **All UNIX Machine** list and select **Filters**.
8. Click **Add Filter**.
9. Type the name and description of the filter and click **Next**.
10. Expand the UNIX data type list, select **Machines - General**, and click **Next**.
11. Select **Basic** and click **Next**.

12. To add more than one operating system to your filter, select **or** for the **Connect the conditions below with** option.
13. Click **Add**, configure the filter, and click **Next**.
    a. In the data property drop-down list, select **OS Name**.
    b. In the operator drop-down list, select **like**.
    c. In the property value text box, type or select the operating systems. You can use % as a wild card. For example, type 'Red Hat%' to include all Linux machines where the operating system begins with Red Hat.
    d. Click **Add** and repeat the process to add another operating system name. For example, 'SUSE%'.
14. Click **Finish**.

    The filter is added to the filter list.
15. Expand your group in the All UNIX Machine list and select **Members**.
16. To immediately update the machine group list, click **Refresh Members**.

    If you do not refresh the members list, the machine group updates in 24 hours or when data is collected from the machines.

What to do next

Schedule the collection of the Linux, UNIX, or Mac OS X data types. See "Schedule Linux, UNIX, and Mac OS X Collections" on page 135.

Schedule Linux, UNIX, and Mac OS X Collections

Scheduled collection jobs run against your Linux, UNIX, and Mac OS X machine group to regularly collect data from the managed machines.

Prerequisites

Create a Linux, UNIX, or Mac OS X machine group, depending on how you want to group and manage your machines. See "Create a Dynamic Machine Group for Linux, UNIX, or Mac OS X Machines" on page 134.

Procedure

1. Click **Administration**.
2. Select **Job Manager > Scheduled**.
3. Click **Add**.
4. Select **Collection** and click **Next**.
5. Type a job name and description and click **Next**.

   For example, Dynamic Linux Collection.
6. Select **Default** filter set and click **Next**.
7. Select your Linux machine group and click **Next**.

   For example, Dynamic Linux Group.
8. Configure when the collection job runs and click **Next**.

   For example, every four hours starting today.
9. Resolve any conflicts and click **Finish**.

   The collection job is added to your Scheduled Jobs list.

What to do next

After a scheduled run time, verify that the job ran successfully. The information is available in Job Manager history for scheduled collections. Select the time and review the general status and success. If the collection was not completely successful, view the machine detail status and resolve any problems.

9 Patching Managed Machines

VCM patch assessment, deployment, and verification ensures continuous security in your environment through proactive compliance of your IT infrastructure. VCM ensures that your managed machines have the latest security patches and other software installed. You can evaluate each physical and virtual managed machine in your environment to ensure that they have the latest supported vendor patches or security bulletins installed, and deploy the recommended patches to those managed machines.

VCM assesses the patch status of Linux and UNIX managed machines, and deploys patches to those machines to ensure compliance in your environment. You can have VCM deploy Linux and UNIX patches without your intervention or you can deploy them manually.

This chapter includes the following topics:

Patch Assessment and Deployment 137
Prerequisite Tasks and Requirements 138
Manually Patching Managed Machines 141
Getting Started with VCM Manual Patching 143
Configuring An Automated Patch Deployment Environment 156
Deploying Patches with Automated Patch Assessment and Deployment 169
How the Linux and UNIX Patch Staging Works 177
How the Linux and UNIX Patching Job Chain Works 178
How the Deploy Action Works 178
Patch Deployment Wizards 179
Running Patching Reports 180

Patch Assessment and Deployment

VCM can deploy patches to 32-bit and 64-bit Linux, UNIX, and Windows managed machines. When you deploy patches on Linux and UNIX machines, follow the best practices defined by the OS vendor.

Supported managed machine types include Red Hat Linux, SUSE Linux, UNIX-based operating systems such as Mac OSX, Solaris, AIX, and HP-UX machines, and Windows machines.

To ensure that Linux, UNIX, and Windows managed machines always include the latest patches, you can have VCM deploy patches to the managed machines when certain events occur in your environment. After you perform the initial configuration for the automatic deployment, no intervention is required to deploy patches to managed machines.

Deploying patches to Linux, UNIX, or Windows managed machines requires the use of a patch assessment template. After you patch Linux, UNIX, or Windows managed machines, VCM runs a delta collection on the patching data for the managed machines to ensure that the next assessment provides the correct patch status.

VCM retains the Linux and UNIX patching change actions in the change log. These actions are available in VCM Compliance and VCM Reports. You can view the patch assessment changes by data type in the Change Management node of the VCM Console. VCM Change Management reports changes on the Patch Assessment and Patch Deployment data types.

VCM 5.7 does not include the Patch Administrator role. If you previously assigned the Patch Administrator role to a user, you must either reassign a different role to the user or let the user know that the role no longer exists.

IMPORTANT For VCM to assess Windows managed machines, you must collect File System, Hot Fix, Registry, and Services data. VCM uses the Hot Fix data to determine which patches are installed on the managed machines. To determine which applications require patches, VCM uses the File System, Registry, and Services data, which must be installed and running. VCM for Linux and UNIX machines collects this data when you perform a patch assessment.

Before you patch Windows 2008 servers and Windows 7 machines, you must verify that the Windows Update service is running. If this service is disabled, the patch deployment fails.

Prerequisite Tasks and Requirements

Before you use VCM to deploy patches to Linux, UNIX, and Windows managed machines, including Solaris machines in single-user mode, you must understand the patch assessment and deployment actions, and perform several prerequisite tasks. VCM runs patch assessments of Linux and UNIX machines against the patches known at the time VCM performs the assessment.

Prerequisites

- To verify whether VCM supports your Linux and UNIX managed machines for patch deployment, see the *VCM Installation Guide*.
- Understand the potential effect of deploying selected patches, and back up critical systems.
- Test all patches before you deploy them to managed machines in your production environment.
- Understand how VCM performs automatic patch deployment to Linux and UNIX managed machines.
- Set Administrator privileges. Users who do not have Administrator privileges to use VCM to deploy patches must have the file-level permissions to the `\\collector_name\cmfiles$\SUM Downloads` share. This default share is shared to everyone with full control, but the file permissions are limited, and the Everyone group has only read permission to the directory. Make sure that the user, or a group to which the user belongs, has write permission to the download directory.

If you encounter problems during automatic or manual patch deployment, see the *VCM Troubleshooting Guide*.

General Requirements

When patching managed machines, be aware of the following requirements.

- You must manage your own patch repository. A temporary expansion of the patches occurs in the /tmp directory. For single-user mode, patches are extracted to /var/tmp. If you do not use the machine group mapping to define an alternate location for the patches, VCM uses the default location of /tmp.
- Store the Linux and UNIX patches in a location that is available locally to the VCM managed machine, such as an NFS mount or a local hard drive. If you store the patches on an NFS mount, you must define the path in machine group mapping in Administration > Settings > General Settings > Patching > Machine Group Mapping. You can use VCM remote commands or another available method to place the patches on the VCM managed machines.
- When you define an alternate location patch repository for a particular machine group, you must select that machine group in VCM before you deploy the patches. If you do not select the machine group, VCM does not acknowledge the alternate location patch repository and does not deploy the patches. The alternate patch location repository appears in the Machine Group Mapping data grid in Administration > Settings > General Settings > Patching > Machine Group Mapping.
- To have VCM deploy patches to groups of managed machines, you must set the machine group mapping to the source location for the patches on the patching repository machine or alternate location machine. Setting the machine group mapping is important when you patch managed machines in single-user mode, because /tmp is not always available. Machine group mappings are not inherited, which means that if you create a machine group under another machine group, the mapping remains separate for each machine group. For example, if you create a machine group called Solaris under the All UNIX Machines machine group, the machine group mapping for All UNIX Machines does not apply to the Solaris machine group.

Location for Linux and UNIX Patches

For automatic patching with VCM 5.7: If you defined a patching repository and a patch staging option, you can submit the job. The optional patch synchronization, staging, and deployment actions occur as scheduled, and the patch download occurs immediately.

For manual patching: When you patch Linux and UNIX machines, you copy the patches to a shared location, then indicate the type of patch deployment and the source location for the patches in the VCM machine group mapping.

Default Location for Linux and UNIX Patches

For automatic patching with VCM 5.7: When you use the VCM 5.7 patch download and optional patch synchronization, staging, and deployment, VCM uses the default locations. If you define other defaults, or if you specify the location in the VCM machine group mapping, VCM stages the patches to that location.

For manual patching: If you do not use the VCM machine group mapping to define an alternate location for the patches, VCM uses the default location of /tmp. A temporary expansion of the patches occurs in the /var/tmp directory, which contains the extracted patches and working files that VCM uses for patch deployment. This custom patch location must have adequate space to accommodate these files, and must be available in single-user mode for VCM to patch Solaris managed machines single-user mode.

VCM retains the Linux and UNIX patching change actions in the change log. These actions are available in VCM Compliance and VCM Reports. You can view the patch assessment changes by data type in the Change Management node of the VCM Console. VCM Change Management reports changes on the Patch Assessment and Patch Deployment data types.

IMPORTANT If a failure occurs at any time during the patch deployment job, the System Administrator must check the status of the system, resolve any issues, then reassess the managed machines. In a job chain, a failure in any step of the job breaks the job chain, which causes all subsequent job steps to not run.

If you encounter problems during automatic or manual patch deployment, see the *VCM Troubleshooting Guide*.

Requirements to Patch Solaris Machines in Single-User Mode

VCM can deploy patches to Solaris machines in single-user mode (run level 1). In this mode, only the system administrator uses the managed machine, and minimal system services are running, such as logins.

To have VCM deploy patches to groups of managed machines, you must set the machine group mapping to the source location for the patches on the patching repository machine or alternate location machine. Setting the machine group mapping is important when you patch managed machines in single-user mode, because `/tmp` is not always available.

Machine group mappings are not inherited, which means that if you create a machine group under another machine group, the mapping remains separate for each machine group. For example, if you create a machine group called Solaris under the All UNIX Machines machine group, the machine group mapping for All UNIX Machines does not apply to the Solaris machine group.

To deploy patches on Solaris machines in single-user mode, you perform several tasks.

Procedure

1. Store the Solaris patches in a local location other than `/tmp` on the target managed machine, that is accessible in single-user mode.

   You can extract the patches in this location, if desired.

2. Verify that the location of `/var/tmp` has adequate disk space for VCM to extract the patches.
3. To set the machine group mapping to the location where you stored the patches, in VCM click **Administration** and select **Settings > General Settings > Patching > Machine Group Mapping**.
4. To have VCM deploy the patches to Solaris managed machines in single-user mode, verify that the `at` daemon is running on the managed machines.

Requirements to Patch Managed Machines Without Changing the Run Level

VCM can deploy patches on Linux and UNIX machines without changing the run level on the managed machine.

To deploy patches on Linux and UNIX machines, you perform several tasks.

Procedure

1. Store the patches in a local location on the target managed machine.

   You can extract the patches in this location, if desired.

   On Solaris machines, do not use the location of `/tmp`, because reboots initiated by the patches clear the content in this directory.

2. Verify that adequate disk space exists on the managed machines for VCM to extract the patches.
   - For Linux and UNIX machines other than Solaris, verify that adequate space exists in `/tmp`.
   - For Solaris machines, verify that adequate space exists in `/var/tmp`.
3. To set the machine group mapping to the location where you stored the patches, click **Administration** and select **Settings > General Settings > Patching > Machine Group Mapping**.
4. To have VCM deploy the patches to Linux and UNIX managed machines where a reboot is required or requested, verify that the `at` daemon is running on the managed machines.

Requirements to Patch AIX Machines

When you use VCM to deploy patches to AIX machines, if the patch prerequisites cannot be resolved by using the downloaded patch bulletin content, some patches might fail. This problem can occur with an AIX patch where the status is StatusNotPatched, and the bulletin details identify a patch dependency on another set of patches whose dependencies cannot be met.

To resolve these patch dependencies on AIX machines, you must determine the patch strategy used for the file sets, Authorized Program Analysis Reports (APARs), Maintenance Level (ML) packages, and Technology Level (TL) packages to be updated.

Although patch dependencies might not appear in the bulletin details, dependencies might exist that cannot be solved. Missing patch prerequisites can occur when some patch versions do not become applicable until after other patches are installed. Maintenance Level (ML) or Technology Level (TL) packages and corresponding bulletins that are intended for upgrades between levels, might not appear as applicable until the ML or TL upgrade is met or exceeded. For example, if you apply a patch that depends on an intermediate ML that is not yet applied, the patch deployment fails because the prerequisite patch dependency was not met.

Manually Patching Managed Machines

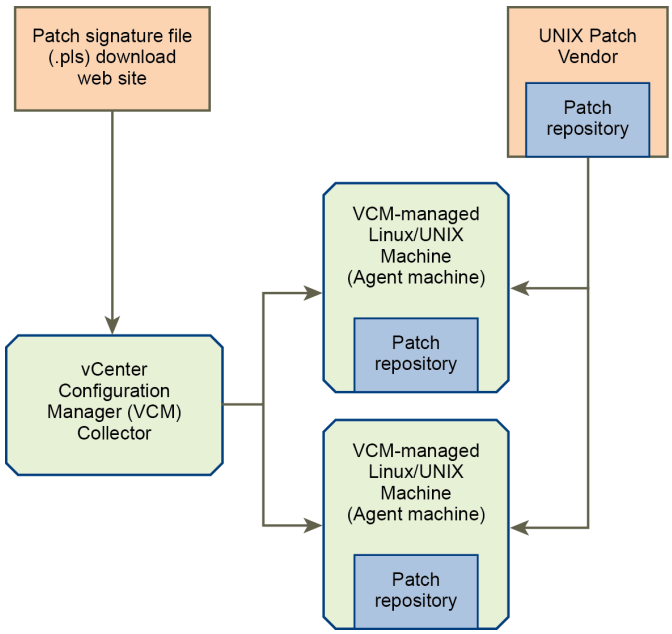
With VCM 5.7, you can manually assess the patch status of Linux, UNIX, and Windows managed machines in your environment and manually deploy patches to managed machines.

With manual patching, the patch assessments of Linux and UNIX machines operate differently from Windows patch assessments.

- Linux and UNIX patch assessments require you to collect new patch assessment data from managed machines before you use VCM to install patches on Linux and UNIX machines. See "Getting Started with VCM Manual Patching for Linux and UNIX Managed Machines" on page 143.
- Windows patch assessments run against data that was previously collected from managed machines. See "Getting Started with VCM Manual Patching for Windows Managed Machines" on page 150.

Manual patching for Linux and UNIX managed machines is illustrated in the following diagram.

Figure 9–1. Manually Patching Managed Machines with VCM



To manually patch Linux and UNIX machines, you can use a Red Hat Linux 6, 64-bit patching repository machine with the Software Content Repository (SCR) Tool installed. You configure the communication protocols on the patching repository machine, download and configure the Software Content Repository (SCR) Tool, and download the patches.

The patches must be accessible to the VCM managed machines by using a method such as an NFS mount to the repository on the Red Hat Linux 6, 64-bit machine where the SCR Tool is installed. See the *Software Content Repository Tool Guide* on the VMware documentation Web site at https://www.vmware.com/support/pubs/vcm_pubs.html.

After you download patches from the vendor Web site, you can use VCM to assess your Linux and UNIX machines. When you are ready to deploy the patches, you use the Deploy action and the machine group mapping in VCM.

To verify whether VCM supports your Linux and UNIX managed machines for patch deployment, see the *VCM Installation Guide*.

With VCM 5.7, you can automate your patching environment. To configure your environment for automated patching with VCM 5.7, see "Configuring An Automated Patch Deployment Environment" on page 156.

VCM uses several types of patching assessment templates to assess the patch state of managed machines.

- Windows patching assessment templates contain one or more bulletins that you use to determine whether the patches that reference the bulletins must be installed on Windows managed machines.
- Linux and UNIX patching assessment templates contain one or more bulletins to filter the patching assessment results.
- User-created assessment templates include one or more bulletins to assess the patch state of Linux, UNIX, or Windows managed machines.
- An imported assessment template, which is a user-created patch deployment utility, associates managed machines with patches for deployment.

Getting Started with VCM Manual Patching

You can use VCM to manually assess the patching state of Linux, UNIX, and Windows managed machines, and manually deploy patches to those machines.

- "Getting Started with VCM Manual Patching for Linux and UNIX Managed Machines" on page 143
- "Getting Started with VCM Manual Patching for Windows Managed Machines" on page 150

To configure your environment for automated patching with VCM 5.7, see "Configuring An Automated Patch Deployment Environment" on page 156.

Getting Started with VCM Manual Patching for Linux and UNIX Managed Machines

Use VCM to manually assess the patch status of Linux and UNIX machines, and deploy patches to those machines.

Linux and UNIX patch assessments require you to collect new patch status data from managed machines. These patch assessments operate differently from VCM patch assessments on Windows managed machines, which run on previously collected data.

To configure your environment for automated patching with VCM 5.7, see "Configuring An Automated Patch Deployment Environment" on page 156.

Prerequisites

- Understand the actions in the patch deployment and perform several prerequisite tasks. See "Prerequisite Tasks and Requirements" on page 138.
- Verify that VCM supports your Linux and UNIX managed machines and operating systems for patch deployment. See the *VCM Installation Guide*.
- Configure the Red Hat patching repository machine. See "Configuring the Patching Repository for Manual Patching" on page 144.

Procedure

1. "Check for Updates to Linux and UNIX Bulletins" on page 144

   To assess the patching state of Linux and UNIX machines, check for updates to patch bulletins.

2. "Create Linux and UNIX Patch Assessment Filters" on page 145

   Patch assessment filters identify patch bulletins that meet user-defined filtering criteria. These filters narrow the scope of bulletins to use in the assessments, which improves the efficiency of the patch assessment.

3. "Collect Patch Assessment Data from Linux and UNIX Machines" on page 145

   To collect Linux and UNIX patch assessment data, you can use bulletins, a patch assessment template, or the Collect wizard.

4. "Review Patch Assessment Results" on page 147

   You can view the results of the patch assessment of Linux and UNIX managed machines.

5. "Deploy Patches to Linux and UNIX Machines" on page 148

   You can use VCM to manually install the patches on Linux and UNIX managed machines.

What to do next

Run patch status reports on Linux, UNIX, and Windows managed machines. See "Running Patching Reports" on page 180.

Configuring the Patching Repository for Manual Patching

To manually patch Linux and UNIX machines, you can use a Red Hat Linux 6, 64-bit patching repository machine with the Software Content Repository (SCR) Tool installed. You configure the communication protocols on the patching repository machine, download and configure the Software Content Repository (SCR) Tool, and download the patches.

The patches must be accessible to the VCM managed machines by using a method such as an NFS mount to the repository on the Red Hat Linux 6, 64-bit machine where the SCR Tool is installed. See the *Software Content Repository Tool Guide* on the VMware documentation Web site at https://www.vmware.com/support/pubs/vcm_pubs.html.

After you download patches from the vendor Web site, you can use VCM to assess your Linux and UNIX machines. When you are ready to deploy the patches, you use the Deploy action and the machine group mapping in VCM.

Prerequisites

- Verify that the Red Hat Linux patching repository machine can access the Internet.
- Locate the *Software Content Repository Tool Guide* on the VMware documentation Web site at https://www.vmware.com/support/pubs/vcm_pubs.html.

Procedure

- To prepare and configure the patching repository machine for use with VCM for manual patching, follow the procedures in the *Software Content Repository Tool Guide*.

  The SCR Tool Guide shows you how to install the required software, configure the patching repository machine, and manage patch content with the SCR Tool.

What to do next

To assess the patching state of Linux and UNIX machines, check for updates to patch bulletins. See "Check for Updates to Linux and UNIX Bulletins" on page 144.

Check for Updates to Linux and UNIX Bulletins

To assess the patching state of Linux and UNIX machines, check for updates to patch bulletins. VCM can manually check for updates on the Internet or from a local file.

VCM downloads new patch signature (`PLS`) files to the VCM Collector.

Prerequisites

- To check for updates on the Internet in the following procedure, verify that the VCM Collector can access the Internet.
- To check for updates using a file on your VCM Collector local file system in the following procedure, copy the patch bulletins to the local machine.

Procedure

1. Click **Patching**.
2. Select ***Linux or UNIX platform*** **> Bulletins > By Bulletin**.
3. Click **Check for Update**, select an update option, and click **Next**.

   VCM locates the bulletins and copies them to your local file system.

What to do next

Identify the patch bulletins collection criteria. See "Create Linux and UNIX Patch Assessment Filters" on page 145.

Create Linux and UNIX Patch Assessment Filters

Patch assessment filters identify patch bulletins that meet user-defined filtering criteria. These filters narrow the scope of bulletins to use in the assessments, which improves the efficiency of the patch assessment.

Procedure

1. Click **Administration**.
2. Select **Collection Filters > Filters**.
3. Click **Add Filter**.
4. Type a name and description for the filter and click **Next**.
5. On the Data Type page, click **UNIX/Linux**.
6. Click **Patch Assessment** and click **Next**.
7. To create a specific set of all available bulletins, on the UNIX Patch Assessment Filters page, click **Include Bulletin(s) that match this criteria**.
8. Use the available settings to define the filter criteria and click **Next**.

   For example: **Platform = Red Hat** and **Severity = Critical**
9. Click **Finish** to create the filter.
10. In the Data Type column of the Collection Filters data grid, locate the Patch Assessment filters, which displays your new filter.

What to do next

Use your new filter when you run a patch assessment. See "Collect Patch Assessment Data from Linux and UNIX Machines" on page 145.

Collect Patch Assessment Data from Linux and UNIX Machines

To collect Linux and UNIX patch assessment data, you can use bulletins, a patch assessment template, or the Collect wizard. VCM runs patch assessments of Linux and UNIX machines against the patches known at the time VCM performs the assessment. During the collection, VCM sends the patch signature `.pls` files to the managed Linux and UNIX machines. You can also schedule Linux and UNIX patch assessments.

Linux and UNIX patch assessments are based on the OS version and machine architecture. When you use templates to collect patch assessment data, you must match the bulletin format to the machine architecture, either 32-bit or 64-bit.

Linux and UNIX patch assessments require you to collect new patch status data from managed machines. These patch assessments operate differently from VCM patch assessments on Windows managed machines, which run on previously collected data.

If you did not collect machine data, the patch assessment results might not appear and the managed machine might not be available for deployment, which would result in a patch-machine mismatch status.

You can view the patch files in the VCM Console under the UNIX tab in the Security, Patches, and Assessment node. Patching changes appear in the Console under the Change Management node, in the Non VCM Initiated and By Machine node.

You can run a patch assessment on managed machines to collect patching data in several ways.

- In the By Bulletin data grid, use the Patch Assessment collection filter.
- In the User-defined Assessment Templates data grid, use a template that filters the patch assessment results.
- In the Collect wizard, use the Patch Assessment Data Class filter. When you use this filter, the VCM Collector sends the `.pls` files to the target machine. The patch signature `.pls` files determine whether required patches are installed on the managed machine. This action might cause a delay. VCM downloads the `.pls` files to the patching repository machine every four hours by default.

Prerequisites

- Verify that the patch assessment finished successfully and that the patch signature files (`.pls`) exist on the VCM Collector.
- Verify that the VCM Agent is installed on the Linux and UNIX managed machines.
- To use filters in the following procedure, verify that you configured filters. See "Create Linux and UNIX Patch Assessment Filters" on page 145.

This procedure uses bulletins to run the patch assessment.

Procedure

1. On the VCM toolbar, click in the **Machine Group** text box, click **All UNIX Machines**, and click **OK**.
2. Click **Patching**
3. Click ***Linux or UNIX platform*** **> Bulletins > By Bulletin**
4. Click **Assess**.
5. In the UNIX Patch Assessment wizard, select **Filters** or **Default Filter**.
   - If you select **Filters**, select the **Patch Assessment Data Class** filter to collect all patch assessment results.
   - If you select **Default Filter**, VCM collects patch assessment data for the managed machines that qualify for the bulletins in the assessment template. If you use another filter for the patch assessment, VCM collects patch assessment data for managed machines that qualify based on the filter settings.
6. Click **Next** and **Finish** to begin the patch assessment on all Linux and UNIX managed machines in the selected machine group.
7. On the toolbar, click **Jobs** and view the progress of the patch assessment collection.

   The patch assessment on Linux and UNIX machines uses the Patch Assessment Data Class collection filter to collect patch data from all machines in the current machine group, and display the results in the Assessment Results node.

8. To view the patch assessment results, click ***Linux or UNIX platform*** and click **Assessment Results > All Bulletins**.

What to do next

Review the results of the patch assessment and obtain the required patches. See "Review Patch Assessment Results" on page 147.

Review Patch Assessment Results

You can view the results of the patch assessment of Linux and UNIX managed machines. The Assessment Results data grid displays the Linux and UNIX machines that VCM assessed, the patch status for each managed machine, and details about the patches.

VCM reports the following patch states.

Icon	Status	Description
	Patched	Patch is applied to the managed machine.
	Patch-Machine Mismatch	Patch OS version or hardware architecture does not match the managed machine.
	Patch Not Needed	Managed machine is up-to-date or the intended software product is not installed on the machine.
	Not Patched	Patch is not applied to the managed machine.
	Not Patched Manual Install	Patch or payload was not found to be defined. During Linux and UNIX patch content download, one or more bulletins did not have payload available. This status can be the result of the patch vendor not supplying a complete patch list for one or more signatures in the patch bulletins. To verify that no patch or payload exists, click **Details** to view the Bulletin Details and verify that no patch is included. Common causes can be that the patch vendor no longer has the patch available for download, such as an old patch that was removed from the vendor download site, or that the patch is not available without a special support agreement, and must be obtained separately from a download by VCM. To remediate the problem, download the content again to obtain the patches or payload, or obtain them manually. To check for bulletin updates and download them, click **Patching**, select **All UNIX/Linux Platforms > Bulletins > By Bulletin**, click **Check for Update**, and finish the wizard.
	Error Occurred	An unexpected condition occurred during the assessment of the managed machine. To determine additional information about the root cause of the exception, run the Debug Event Viewer at `C:\Program Files (x86)\VMware\VCM\Tools\ecmDebugEventViewer.exe`.
	Signature Not Found	Patch signature `.pls` file does not exist on the managed machine and the patch status cannot be determined.

Icon	Status	Description
	Incorrect MD5	MD5 Hash generated from the patch signature (`PLS`) file, which contains the content and signature, does not match the expected value on the Linux or UNIX managed machine. Be aware that MD5 is NOT validated against the vendor MD5 hash data.
	Patch Status Unknown	Patch status of the managed machine cannot be determined.
	Not patched by exception	If patch assessment results conform to the patching exception definition, VCM does not patch the managed machine, and changes the results from not patched to patched. The exception can be temporary or permanent.
	Patched by exception	If patch assessment results conform to the patching exception definition, VCM patches the managed machine and updates the results to patched. The exception can be temporary or permanent.
	Patch not applicable	If patch assessment results conform to the patching exception definition, VCM does not patch the managed machine, and changes the results from not patched to patched. The exception can be temporary or permanent.
	User-defined exception	If patch assessment results conform to the patching exception definition, VCM does not patch the managed machine, and updates the result to the user-defined reason for the patch status. You can type a description in the text box or select the status from a list of previous user-defined patch status reasons. The exception can be temporary or permanent.

Prerequisites

Use FTP, NFS, or a premounted file system to acquire and store the Linux and UNIX patches.

Procedure

1. Click **Patching**.
2. To display the patch status for all machines that were assessed, click ***Linux or UNIX platform***and select **Assessment Results > All Bulletins**.
3. To display the assessment results for a single bulletin, select **By Specific Bulletin** and select a bulletin in the center pane.
4. Review the patch status for each managed machine.

   VCM reports the patch states.

If you did not collect machine data, the patch assessment results might not appear and the managed machine might not be available for deployment, which would result in a patch-machine mismatch status.

What to do next

Deploy patches. See "Deploy Patches to Linux and UNIX Machines" on page 148.

Deploy Patches to Linux and UNIX Machines

You can use VCM to manually install the patches on Linux and UNIX managed machines.

The patch deployment assesses whether the patch was installed on the VCM managed machines.

IMPORTANT If a failure occurs at any time during the patch deployment job, the System Administrator must check the status of the system, resolve any issues, then reassess the managed machines. In a job chain, a failure in any step of the job breaks the job chain, which causes all subsequent job steps to not run.

Prerequisites

- Verify that your Linux and UNIX managed machines and operating systems are supported for patch deployment. See the *VCM Installation Guide*.
- View the assessment results to verify that the patch assessments ran successfully.
- Verify that patches are available locally to the managed machines.
- Perform the prerequisite tasks. See "Prerequisite Tasks and Requirements" on page 138.

You can deploy patches from the assessment results for all bulletins, a user-created assessment template, or an imported template. This procedure uses the Deploy wizard in the All Bulletins node to deploy the patches.

Procedure

1. Click **Patching** and select ***Linux or UNIX platform*** **> Assessment Results > All Bulletins**.
2. Select the patches for VCM to deploy to managed machines.
3. Click **Deploy**.
4. Review the Recommend Action and Data Age, and select the machines and patches to deploy.

   The data age is the number of days since the patch assessment was run on the managed machine. The data age reflects the last time you collected patch assessment data from managed machines using the Unix Patch Assessment data class with filters, a filter set or a filter set group, or ran a patch assessment template.
5. Review the required patch list.
6. (Optional) To set the run level for the patch installation on Solaris managed machines, click **Install patches in single-user mode (run level 1 or S)**.

   In single-user mode, a network is not available.
7. To review and update the command-line options and remote commands, click **Advanced**.
   a. (Optional) To override the command-line options used to deploy the patches, type the command in the platform type text box.
   b. (Optional) To specify a pre-deployment remote command, select the **Enable pre-deployment Remote Command** check box and type the command in the text box, or click the ellipsis and select an existing remote command.
   c. (Optional) To specify a post-deployment remote command, select the **Enable post-deployment Remote Command** check box and type the command in the text box, or click the ellipsis and select an existing remote command.
   d. (Optional) To run the remote commands in the managed machine's current run level or in the run level, select the appropriate run level option, click **OK**, and click **Next**.
8. If you selected multiple patches to deploy, verify that the order of patches is correct, or reorder them and click **Next**.
9. Select the staging option and set the schedule for the patch deployment job and click **Next**.

a. Select **Stage patches manually**, and set the time and date for patch staging.

b. Select whether to have VCM deploy the patches to target managed machines immediately or later, and set the time and date for patch deployment.

10. Set the reboot schedule options and click **Next**.

    a. Select whether to reboot the managed machine after VCM installs the patches.

    b. If you have VCM reboot the machine, set the reboot message and delay.

11. Confirm the patch deployment summary and click **Finish** to deploy the patches.

    After you deploy the patches, VCM collects patch assessment data again to confirm that the patches were applied.

12. In the user-defined assessment template data grid, click **Assess** to run another patch assessment, and verify that the patch status is Patched in the assessment results for the patched managed machines.

    If a managed machine is in a pending reboot state, the patch status for the machine is Not Patched.

What to do next

- For more information about using the Deploy wizard and scheduling patch deployments for Windows managed machines, see the online help.
- To view the status of the patch deployment job, click **Patching** and select **Job Management > UNIX > Job Manager > Running**.
- If you scheduled the job to run later, to view the status of the scheduled deployment, click **Patching** and select **Job Management > UNIX > Job Manager > Scheduled > Deployments**.
- VCM retains the Linux and UNIX patching change actions in the change log. These actions are available in VCM Compliance and VCM Reports. You can view the patch assessment changes by data type in the Change Management node of the VCM Console. VCM Change Management reports changes on the Patch Assessment and Patch Deployment data types.

Getting Started with VCM Manual Patching for Windows Managed Machines

Use VCM to manually assess the patch status of Windows managed machines, and deploy patches to those machines.

To configure your environment for automated patching with VCM 5.7, see "Configuring An Automated Patch Deployment Environment" on page 156.

Prerequisites

To deploy patches to Windows managed machines, you must understand patch deployment actions and perform several prerequisite tasks. See "Prerequisite Tasks and Requirements" on page 138.

Procedure

1. "Check for Updates to Windows Bulletins" on page 151

   Use VCM to check for updates to patch bulletins on the Internet, which you can use in patch assessments of managed machines to enforce compliance.

2. "Download Patches for Windows Patch Deployment" on page 152

   You can download patches for deployment to Windows managed machines based on the bulletins included in a patch assessment template.

3. "View Windows Bulletin Details" on page 152

   You can view detailed information about Windows patch bulletins, including technical details, recommendations, and whether a reboot of the managed machine is required.

4. "Collect Data from Windows Machines by Using the VCM Patching Filter Sets" on page 153

   To obtain the current patch status of Windows managed machines, collect patch data from those machines. VCM requires that you collect current information about the File System, Hotfixes, Registry, and Services Windows data types.

5. "Assess Windows Machines" on page 153

   To assess the patch status of Windows machines, use a patching assessment template.

6. "Review Windows Patch Assessment Results" on page 154

   You can use the Assessment Results data grid to display the Windows machines that VCM assessed, the patch status for each machine, and details about the patches.

7. "Deploy Patches to Windows Machines" on page 155

   You can deploy patches to Windows machines that are managed by VCM.

8. "Collect Data from Windows Machines by Using the VCM Patching Filter Sets" on page 153

   After you deploy patches, to obtain the updated patch status of Windows managed machines, collect patch data again from the managed machines.

9. "Assess Windows Machines" on page 153

   After you collect data, run another patch assessment to assess the updated patch status of Windows machines.

What to do next

Run patch status reports on Linux, UNIX, and Windows managed machines. See "Running Patching Reports" on page 180.

Check for Updates to Windows Bulletins

Use VCM to check for updates to patch bulletins on the Internet, which you can use in patch assessments of managed machines to enforce compliance.

Procedure

1. Click **Patching**.
2. Select **Windows > Bulletins**.
3. To display a comprehensive view of all released bulletins, click **By Bulletin**.
4. To find a bulletin for an installed software product, click **By Affected Product**.
5. Click **Check for Update**.
6. If updates exist, download the updates.

   Follow the prompts to update your bulletins, force an update to the bulletins, or cancel the request.

7. Click **Finish** to submit the download job to the pending job queue.

   When the job is finished running, the content is available in VCM.

What to do next

Download patches for deployment. See "Download Patches for Windows Patch Deployment" on page 152.

Download Patches for Windows Patch Deployment

You can download patches for deployment to Windows managed machines based on the bulletins included in a patch assessment template.

When you download patches, VCM first determines whether the patches exist on the VCM Collector, then checks the download Web site. If VCM finds the patches, you can download them. If VCM does not find the patches on the Collector or the Web site, you must locate the patches and download them.

IMPORTANT Users who do not have Administrator privileges to use VCM to deploy patches must have the file-level permissions to the `\\collector_name\cmfiles$\SUM Downloads` share. This default share is shared to everyone with full control, but the file permissions are limited, and the Everyone group has only read permission to the directory. Make sure that the user, or a group to which the user belongs, has write permission to the download directory.

Prerequisites

Verify that users who do not have Administrator privileges to use VCM to deploy patches have file-level permissions to the `\\collector_name\cmfiles$\SUM Downloads` share.

Procedure

1. Click **Patching** and select **Windows > Assessment Templates**.
2. To view the status of the bulletin and whether the bulletin is superseded, click **Details**.
3. In the Assessment Templates toolbar, click **Download Patches** to locate the patch files on the Internet and download them to the VCM Collector.

   The default download directory is: `\Program Files (x86)VMware\VCM\WebConsole\L1033\Files\SUM Downloads`. This directory is shared as `\\collector_name\cmfiles$\SUM Downloads`.
4. (Optional) To configure an alternate location to store the patches for staging to the managed machine, click **Administration**, select **Settings > General Settings > Patching > Machine Group Mapping**, and edit the **Local Patch Path**.

   The VCM service synchronizes files between the SUM Downloads directory and the specified paths on alternate location machines.

What to do next

Review the technical details, recommendations, and reboot information about Windows patch bulletins. See "View Windows Bulletin Details" on page 152.

View Windows Bulletin Details

You can view detailed information about Windows patch bulletins, including technical details, recommendations, and whether a reboot of the managed machine is required.

Procedure

1. Click **Patching**and select **Windows > Bulletins > By Bulletin.**
2. Select a bulletin.
3. To view the technical details about the bulletin, click **Details**.
4. In the Bulletin Details window, under **On the Web**, click the link to view additional information about the bulletin on the Internet.

What to do next

Use filter sets to collect data from Windows managed machines. See "Collect Data from Windows Machines by Using the VCM Patching Filter Sets" on page 153.

Collect Data from Windows Machines by Using the VCM Patching Filter Sets

To obtain the current patch status of Windows managed machines, collect patch data from those machines. VCM requires that you collect current information about the File System, Hotfixes, Registry, and Services Windows data types.

After the patch deployment, collect patch data again from the managed machines.

Procedure

1. On the toolbar, click **Collect**.
2. Select the Windows machines from which to collect data.
3. Click **Select a Collection Filter Set to apply to these machines** and click **Next**.
4. Select the **Patching - Windows Security Bulletins** filter set and click **Next**.

   This filter set gathers information for all available Windows security bulletins that you can use to patch Windows machines. Select any monthly filter set to filter the bulletins released in a particular month.
5. If no conflicts appear, click **Finish** to begin the collection.

   If problems occur during data collection when you use the VCM patching filter sets and the default Network Authority Account, either give the account access to the Windows servers, or use a separate Network Authority Account for these machines. For more information, see Default Network Authority Account .

What to do next

Use a patching assessment template to assess the patching state of managed machines. See "Assess Windows Machines" on page 153.

Assess Windows Machines

To assess the patch status of Windows machines, use a patching assessment template. After you deploy patches to managed machines and collect updated patch data, run another patch assessment to assess the updated patch status of Windows machines.

Because the assessment is run only against data in the VCM database, you must collect patching data from managed machines before and after you run an assessment. When run, the assessment template checks the data collected from managed machines to verify whether the patches that the bulletins reference must be installed on those machines. For example, a template might contain all bulletins related to Internet Explorer 9 to ensure that all of the installed instances have the latest security fixes.

The patch assessment checks all of the managed machines in the active machine group. A patch deployment applies only to the machines in the machine group that are managed by VCM.

You can create an assessment template based on bulletins or affected software products, or by importing a text file that lists machines that require a particular patch or that lists machine and patch pairs. This procedure generates an assessment template based on bulletins.

Prerequisites

Review the collected patching data and determine which managed machines must be patched.

Procedure

1. Click **Patching** and select **Windows > Bulletins > By Bulletin**.
2. Select a bulletin.
3. Click **Details**, read the technical details for the affected products and vendor recommendations, and read the deployment summary to identify any issues that might interfere with the distribution of the bulletin.
4. Click **On the Web** to link to vendor information about the bulletin.
5. Review all of the bulletins to include in the assessment template.
6. To create an assessment template that includes all of the bulletins for the patches to deploy, select all of the relevant bulletins and click **Create Template**.
7. Verify that the bulletins are selected and click **Finish** to create the template.
8. On the VCM toolbar, verify that the correct machine group is selected.
9. Click **Patching** and select **Windows > Assessment Templates**.
10. Select the template to run and click **Assess**.
11. When the assessment finishes, click the **Refresh** button on the toolbar and view the assessment results in the data grid.

What to do next

Review the results of the patch assessment. See "Review Windows Patch Assessment Results" on page 154.

Review Windows Patch Assessment Results

You can use the Assessment Results data grid to display the Windows machines that VCM assessed, the patch status for each machine, and details about the patches.

Prerequisites

Run a patch assessment template.

Procedure

1. Click **Patching**.
2. Select **Windows > Assessment Templates**
3. Select the template and view the results in the data grid.
4. View the Patch Status column to determine the state of each managed machine for the patches listed.
5. If the assessment results provide multiple pages of data, click the **Patch Status** column heading and drag it up to **Column Grouping**.
6. In the Column Grouping view, expand the **Not Patched** status to view all of the managed machines that are not patched.
7. To display the graphical representation of the patch assessment status, select **Enable/Disable Summary** in the template data grid view to enable the Summary view.
8. Click the assessment template node.

   The Summary view displays a graph of the patch status for the managed machines that were assessed and the patch status by asset classification and bulletin severity rating.

The Not Patched column displays machines that require a patch or a reboot for an applied patch.

From the Summary view, you can navigate to the affected managed machines.

What to do next

Deploy patches. See "Deploy Patches to Windows Machines" on page 155.

Deploy Patches to Windows Machines

You can deploy patches to Windows machines that are managed by VCM. These machines appear in the Licensed Machines node in VCM Administration Machines Manager.

IMPORTANT If a failure occurs at any time during the patch deployment job, the System Administrator must check the status of the system, resolve any issues, then reassess the managed machines. In a job chain, a failure in any step of the job breaks the job chain, which causes all subsequent job steps to not run.

Prerequisites

- Follow the patching guidelines. See "Prerequisite Tasks and Requirements" on page 138.
- Before you patch Windows 2008 servers and Windows 7 machines, verify that the Windows Update service is running, which means that it is set to something other than Disabled.

Procedure

1. Click **Patching**.
2. Select **Windows > Assessment Templates** and select the template used for the assessment.
3. Make sure that the data grid view is visible so that you can view the managed machines and bulletins.
4. Locate the rows that display the StatusNotPatched status.

   To identify the managed machines that must be patched, drag a column header up to the Column Grouping area to group the Patch Status column.
5. Highlight the row that contains the managed machine to be patched and click **Deploy**.

   With VCM Service Desk Integration installed, the Service Desk Connector dialog box appears before the VCM patching Deploy wizard. VCM Orchestrator must approve the deployment job before it can run.
6. (Optional) Select additional machine and patch combinations to include.
7. Select the managed machines and patches to deploy and click **Next**.

   To detect the patch, the Deploy wizard checks the Collector first, and uses the downloaded patch, if found. If patches are not found, the Deploy wizard attempts to locate the patch on the Internet.

   If the patch is found on the Internet, you can download the patch immediately or at run time.

   If access to the Internet is denied, you must obtain the patches manually and store them in `\\collector_name\cmfiles$\SUM Downloads` on the VCM Collector.
8. If you selected multiple patches to deploy, confirm the order in which to deploy the patches or reorder them, and click **Next**.
9. On the Switches page, do not select any switches for the installation, and click **Next**.
10. On the Patch Staging and Deployment Schedule page, select to copy the patches to the VCM managed machine during deployment, select to run the deployment immediately or schedule it to run later, and click **Next**.

11. Click **Next** again to either schedule the deploy job or to instruct VCM to run the job immediately.
12. On the Reboot Options page, select to not reboot the machine and click **Next**.
13. On the confirmation page, click **Finish** to deploy the patch.

    When the deployment finishes, VCM runs a delta collection of the Patching Security Bulletins filter set to update the assessment information.
14. In the assessment template data grid view, run another assessment and confirm that the machines you patched are marked as Patched in the assessment results.

    If a machine is in a pending reboot state, the patch status for the machine is Not Patched.

What to do next

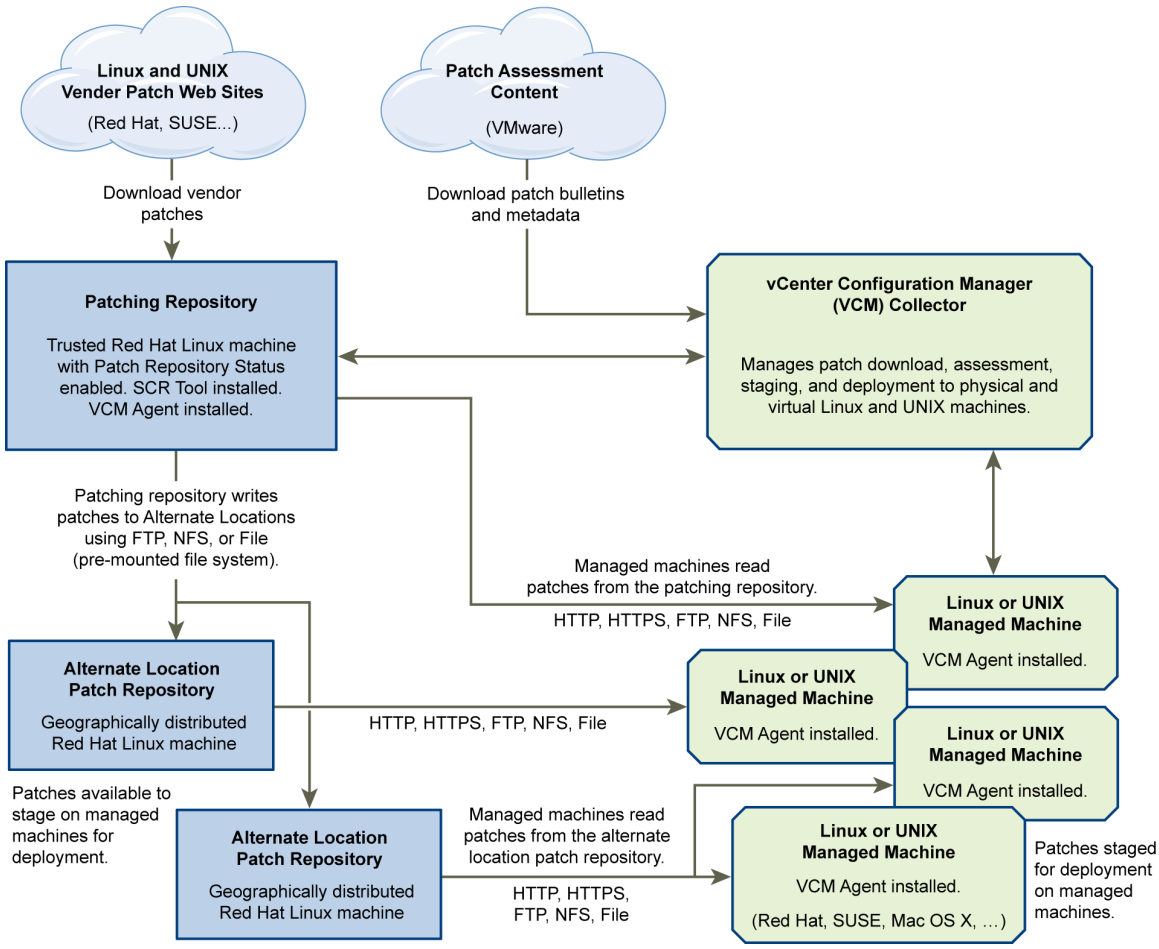
- For more information about scheduling patch deployments for Windows managed machines, see the online help.
- To view the status of the patch deployment job, click **Patching** and select **Job Management > Windows > Job Manager > Running**.
- If you scheduled the job to run later, to view the status of the scheduled deployment, click **Patching** and select **Job Management > Windows > Job Manager > Scheduled > Deployments**.
- VCM retains the Windows patching change actions in the change log. These actions are available in VCM Compliance and VCM Reports. You can view the patch assessment changes by data type in the Change Management node of the VCM Console. VCM Change Management reports changes on the Patch Assessment and Patch Deployment data types.

Configuring An Automated Patch Deployment Environment

To automate the patching of Linux, UNIX, and Windows managed machines in your environment, you configure the patching repository and optional alternate location machines used to store and distribute the patches, either geographically or across firewalls. Automated patching includes both event-driven and scheduled patch assessment and deployment. After you configure the environment, no additional intervention is required to deploy the patches to managed machines.

When managed machines are distributed geographically or by firewalls in a Linux and UNIX environment, VCM supports primary and secondary patch repositories to store patches for staging and deployment to target managed machines. The primary patching repository Red Hat Linux machine has the Software Content Repository (SCR) Tool and the VCM Agent installed. One or more geographically distributed alternate location Red Hat Linux machines serve as secondary patch repositories that VCM uses to patch managed machines.

Figure 9–2. Automatic Patching of Linux and UNIX Managed Machines with VCM


Linux and UNIX Vender Patch Web Sites
(Red Hat, SUSE...)
Patch Assessment Content
(VMware)
Download vendor patches
Download patch bulletins and metadata
Patching Repository
Trusted Red Hat Linux machine with Patch Repository Status enabled. SCR Tool installed. VCM Agent installed.
vCenter Configuration Manager (VCM) Collector
Manages patch download, assessment, staging, and deployment to physical and virtual Linux and UNIX machines.
Patching repository writes patches to Alternate Locations using FTP, NFS, or File (pre-mounted file system).
Managed machines read patches from the patching repository.
HTTP, HTTPS, FTP, NFS, File
Linux or UNIX Managed Machine
VCM Agent installed.
Alternate Location Patch Repository
Geographically distributed Red Hat Linux machine
HTTP, HTTPS, FTP, NFS, File
Linux or UNIX Managed Machine
VCM Agent installed.
Linux or UNIX Managed Machine
VCM Agent installed.
Patches available to stage on managed machines for deployment.
Alternate Location Patch Repository
Geographically distributed Red Hat Linux machine
Managed machines read patches from the alternate location patch repository.
HTTP, HTTPS, FTP, NFS, File
Linux or UNIX Managed Machine
VCM Agent installed.
(Red Hat, SUSE, Mac OS X, ...)
Patches staged for deployment on managed machines.

Prerequisites

Understand the patch assessment and deployment actions, and perform the prerequisite tasks. See "Prerequisite Tasks and Requirements" on page 138.

Procedure

1. "Configuring the Patching Repository Machine" on page 158

   To patch managed Linux and UNIX machines, you must install a Red Hat Linux 6, 64-bit machine as the patching repository, configure the communication protocols, and download and configure the Software Content Repository (SCR) Tool.

2. "(Optional) Configuring the Alternate Location Patch Repository Machines" on page 161

   To patch managed machines in a distributed patching environment, you configure one or more Red Hat Linux 6, 64-bit machines as alternate location patch repositories to store copies of the Linux and UNIX patches for VCM to deploy to managed machines.

3. "Configuring VCM to Work with the Patching Repository and Alternate Locations" on page 162

   You must configure VCM to work with the patching repository and optional alternate location patch repository machines.

4. "Deploying Patches with Automated Patch Assessment and Deployment" on page 169

To ensure that Linux, UNIX, and Windows managed machines always include the latest patches, you can have VCM deploy patches to the managed machines when certain events occur in your environment. After you perform the initial configuration for the automatic deployment, no intervention is required to deploy patches to managed machines.

5. "Configure VCM for Automatic Scheduled Patch Assessment and Deployment" on page 176

   To ensure that Linux, UNIX, and Windows managed machines are updated with the latest patches on a regular basis, you can schedule VCM to deploy patches to the managed machines. The automatic scheduled patch assessment and deployment matches a machine group to a patch assessment template.

What to do next

- For Linux and UNIX patching, after a job triggers, view the job chain in the VCM Job Manager, and the finished job chain jobs in Job Manager History. See "How the Linux and UNIX Patching Job Chain Works" on page 178.
- (Optional) You can schedule an automatic patch deployment. See "Configure VCM for Automatic Scheduled Patch Assessment and Deployment" on page 176.

Configuring the Patching Repository Machine

To patch managed Linux and UNIX machines, you must install a Red Hat Linux 6, 64-bit machine as the patching repository, configure the communication protocols, and download and configure the Software Content Repository (SCR) Tool.

CAUTION To ensure security in a geographically distributed Linux and UNIX patching environment, the credentials that you use to transfer patches from the patching repository to the alternate location must be different from the credentials that you use to copy patches from the alternate location to the target managed machines. The credentials used to transfer patch files to the alternate location must have read and write privileges. Use read-only credentials to stage patches from an alternate location to a managed machine.

If you already configured the Red Hat Linux patching repository machine for manual patching with VCM, you can skip this procedure.

Prerequisites

- Verify that the Red Hat Linux patching repository machine can access the Internet.
- When you set up a patching repository machine and alternate location machines, you must ensure that users have proper permissions and protocols configured to read patches from the patching repository machine and write patches to the alternate location machines. See "Communication Protocols to Stage Linux and UNIX Patches" on page 159.
- Decide which protocol to use to copy patches from the patching repository machine to the optional alternate location machines. To configure the protocol, see http://kb.vmware.com/kb/2051632 and the Red Hat Linux information online.

Procedure

1. Download and install the latest version of Java and the Oracle Java Cryptography Extension (JCE), which is used for Software Content Repository (SCR) Tool password encryption.
2. Install the VCM 5.7 Linux Agent on the patching repository machine. See the VCM online help.
3. Install and configure the service that supports the desired communication method used by the managed machines.
4. Configure the communication protocol.

What to do next

- Download the Software Content Repository (SCR) Tool 5.0. See "Download the Software Content Repository Tool" on page 159.
- Configure the SCR Tool. See "Configure the SCR Tool" on page 160.

Communication Protocols to Stage Linux and UNIX Patches

VCM supports patching managed machines in distributed environments, either geographically or separated by firewalls. VCM uses a single Red Hat Linux patching repository machine that has the Software Content Repository (SCR) Tool installed. The distributed patching configuration can include one or more Red Hat Linux alternate location machines to store the patches for deployment to managed machines.

Before you copy Linux and UNIX patches from the patching repository machine to alternate location machines or to target managed machines, you must configure the protocols to enable the communication between the patching repository, alternate locations, and managed machines. The copy operations use several protocols.

- For the patching repository to copy patches to alternate locations, use SFTP, SCP, FTP, NFS, or a premounted file system.
- For target managed machines to retrieve the patch files from the patching repository, use HTTPS, HTTP, FTP, NFS, or a premounted file system.
- For target managed machines to retrieve the patch files from the alternate locations, use HTTP, NFS, HTTPS, FTP, or a premounted file system.

You can configure HTTP, FTP, and other supported protocols on the Red Hat Linux patching repository and alternate location machines.

CAUTION When you use HTTP or HTTPS to stage patches from the patching repository to Solaris managed machines, the staging action might consume all of the swap space in `/tmp`, to the full file size of the patch, which might be an issue on production machines.

For more information to configure the protocols, see http://kb.vmware.com/kb/2051632.

Download the Software Content Repository Tool

The Software Content Repository (SCR) Tool is a standalone Java software application that is installed on the patching repository machine. VCM uses the SCR Tool to download Linux and UNIX patches from OS vendor Web sites to the patching repository, and deploys these patches to Linux and UNIX managed machines.

To obtain Linux and UNIX patches from vendor Web sites, download the SCR Tool from the Download VMware vCenter Configuration Manager Web site.

Prerequisites

Verify that you can access the VCM documentation page at https://www.vmware.com/support/pubs/vcm_pubs.html.

Procedure

1. On the VCM documentation page, click **Current Product Download**.
2. On the Download VMware vCenter Configuration Manager Web site, click **Drivers & Tools**.
3. Expand **VMware vCenter Configuration Manager Tools**.
4. For your VCM version, click **Go to Downloads**.
5. To download and run the Software Content Repository Tool, click **Download Manager** or **Manually Download**.

What to do next

Configure the SCR Tool for Linux and UNIX Patching. See "Configure the SCR Tool" on page 160.

Configure the SCR Tool

VCM 5.7 patching for Linux and UNIX requires the Software Content Repository (SCR) Tool. To support the use of the SCR Tool, VCM uses the properties files for the Linux and UNIX platforms.

The properties files include the environment settings that the SCR Tool uses to download the patch content for each supported Linux and UNIX platform. For information about the `.plp` files, see the *Software Content Repository (SCR) Tool Guide*.

To integrate the SCR Tool with VCM, you must place a special bundle of properties files for the platforms in a specific directory on the patching repository machine. The properties file names use the format *`platform`*`-rt.properties`.

When you submit a patch download job in VCM, during patch deployment VCM reads a special bundled runtime file and uses the content in it to create additional required files. When you edit the special bundled runtime properties files in the following procedure, you must ensure the following restrictions on the runtime properties files.

- Must not contain relative paths.
- Must have credentials and proxy information as defined in the *Software Content Repository (SCR) Tool Guide*.

Prerequisites

- Locate the *Software Content Repository Tool Guide* on the VMware documentation Web site for use in the following procedure. See https://www.vmware.com/support/pubs/vcm_pubs.html.
- Download the Java Runtime Environment (JRE) to support the SCR Tool on the patching repository machine. See the *Software Content Repository Tool Guide*.
- Download and install the Java Cryptography Extension (JCE) on the patching repository Red Hat Linux machine where the SCR Tool is installed. See the *Software Content Repository Tool Guide*.
- Obtain the special bundle of properties files, `Sample-SCR-Properties.tgz`, at the same location where you downloaded the SCR Tool.
- Install the SCR Tool on the RedHat Linux 6, 64-bit patching repository machine, and do not modify the properties files.

Procedure

1. On the patching repository machine, download the runtime properties files tarball from the same Web site where you downloaded the SCR Tool tarball or zip file.
2. Extract the contents of the runtime properties tarball into the `/SCR/conf` directory.

   The properties files must be named as follows.

   - `AIX-rt.properties`
   - `HPUX-rt.properties`
   - `logging.properties`
   - `MAC-rt.properties`
   - `SOLARIS-rt.properties`
   - `REDHAT-rt.properties`
   - `SUSE-rt.properties`
3. To modify the runtime properties files that you extracted from the tarball, use the *Software Content Repository Tool Guide*.

IMPORTANT Do not change the file names of the extracted runtime properties files.

What to do next

Configure the Red Hat Linux alternate location repository machines, including the communication protocol. See "(Optional) Configuring the Alternate Location Patch Repository Machines" on page 161.

(Optional) Configuring the Alternate Location Patch Repository Machines

To patch managed machines in a distributed patching environment, you configure one or more Red Hat Linux 6, 64-bit machines as alternate location patch repositories to store copies of the Linux and UNIX patches for VCM to deploy to managed machines.

To determine which alternate location to use to copy patches to the managed machines, VCM uses the machine group mapping. The alternate location machine does not require the VCM Agent to be installed. The VCM Agent on the target managed machine obtains the patches from the alternate location machines.

CAUTION To ensure security in a geographically distributed Linux and UNIX patching environment, the credentials that you use to transfer patches from the patching repository to the alternate location must differ from the credentials that you use to copy patches from the alternate location to the target managed machines. The credentials used to transfer patch files to the alternate location must have read and write privileges. Use read-only credentials to stage patches from an alternate location to a managed machine.

Prerequisites

- When you set up a patching repository machine and alternate location machines, you must ensure that users have proper permissions and protocols configured to read patches from the patching repository machine and write patches to the alternate location machines. See "Communication Protocols to Stage Linux and UNIX Patches" on page 159.
- Decide which protocol to use to copy patches from the alternate location machines to the target managed machines. To configure the protocol, see http://kb.vmware.com/kb/2051632 and the Red Hat Linux information online.

Follow this procedure for each Red Hat Linux alternate location patch repository machine in your environment.

Procedure

1. On the Red Hat Linux alternate location machine, configure the protocol to receive patches from the patching repository machine.
2. Configure the protocol to communicate with the target managed machines so that the managed machines can copy patches from the alternate location machines.

What to do next

Configure VCM. See "Configuring VCM to Work with the Patching Repository and Alternate Locations" on page 162.

Configuring VCM to Work with the Patching Repository and Alternate Locations

The distributed Linux and UNIX patching environment includes a Red Hat Linux patching repository machine and the VCM Collector. Optionally, you can include one or more geographically distributed alternate location machines. VCM uses the patching repository and the alternate locations to store patches and stage them to Linux and UNIX managed machines for patch deployment.

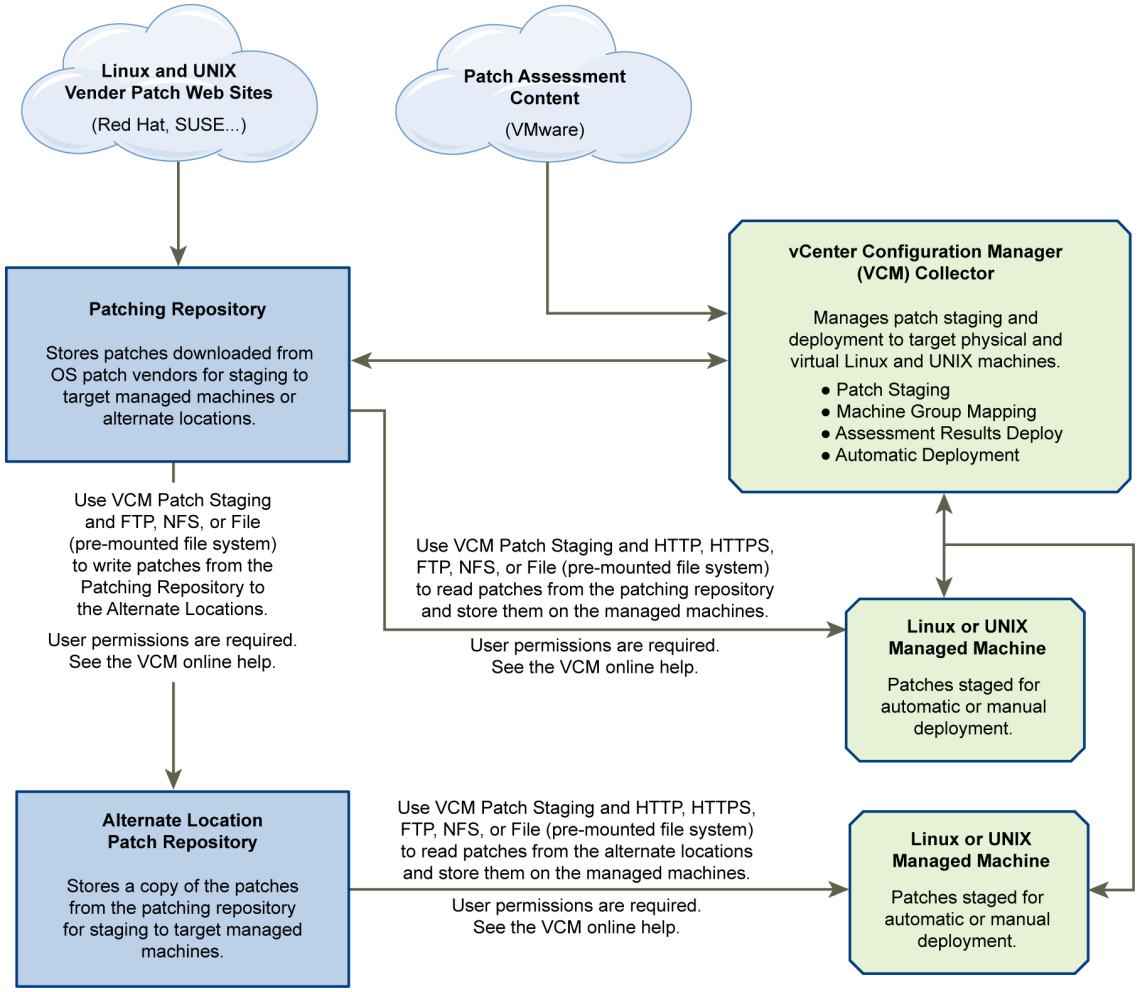
VCM supports distributed patching environments with the use of a single patching repository machine and one or more alternate location machines to store replications of the patches for automatic and manual patch deployment to managed machines.

A physical or virtual machine is potentially a patching repository machine if it is a Red Hat Linux machine that has the VCM 5.7 Linux Agent and the Software Content Repository (SCR) Tool 5.0 installed. The Red Hat Linux machine that you designate as the patching repository machine must be configured as a trusted machine in **Administration > Certificates** and must have the Patching Repository status assigned to it to elevate its status as a trusted machine for security purposes.

All target managed machines to be patched must be trusted machines, if they require credentials to obtain patch payload from the patching repository or a geographically distributed alternate location.

To patch managed machines in a geographically distributed patching environment, you configure a separate Red Hat Linux machine to be the alternate location patching repository for that environment.

Figure 9–3. Staging Linux and UNIX Patches on VCM Managed Machines



To simplify the configuration for how Linux and UNIX managed machines obtain and extract patches during patch staging and deployment, you map machine groups and network locations. To stage and deploy the patches to target managed machines, you select a patching repository or an alternate location machine. See the VCM online help.

You define a Linux and UNIX patch staging configuration for the patching repository and the geographically distributed alternate location machines. Managed machines use the patch staging configuration to obtain the patches for VCM to deploy to managed machines.

Configure VCM

You must configure VCM to work with the patching repository and optional alternate location patch repository machines.

Prerequisites

- Configure the Red Hat Linux patching repository machine, including the communication protocol. See "Configuring the Patching Repository Machine" on page 158.
- (Optional) Configure one or more alternate location patching repository machines, including the communication protocol. See "(Optional) Configuring the Alternate Location Patch Repository Machines" on page 161.

- Verify that the machine groups to be used for Linux and UNIX patching are defined in VCM, and add any new machine groups for VCM to patch specific groups of managed machines. See the VCM online help.
- (Optional) If your VCM Collector is not configured to use HTTPS, before you add a patch staging configuration you must allow the Collector to bypass the HTTPS setting. Select **Administration > Settings > General Setting > Collector**. Change the value of the setting named `Allow HTTP communication (HTTPS bypass) when entering sensitive parameter values` to **Yes**.

Procedure

1. "Enable the Trust and Patching Status for the Patching Repository Machine" on page 164

   You must enable the trust and patching repository status for the Red Hat Linux patching repository machine, to designate it as a trusted patching machine for security purposes.

2. "Configure How Managed Machines Stage Patches for Deployment" on page 165

   For VCM to stage the Linux and UNIX patches and deploy them to managed machines, select a patching repository machine and an optional geographically distributed alternate location machine.

3. "Configure the Machine Group Mapping to Use the Patch Staging Configuration" on page 167

   You must configure the machine group for VCM to use to deploy Linux and UNIX patches to target managed machines. You can combine Linux and UNIX managed machines into a single machine group, and have VCM use a single action to deploy the patches to all of the managed machines in that group.

4. "Verify the SCR Tool Base Path for the Patching Repository" on page 168

   The setting for the Software Content Repository (SCR) Tool base path in VCM must point to the location where you installed the SCR Tool on the patching repository machine.

What to do next

- Run a patch assessment on the managed machines that are targeted for patch deployment, examine the results. See the VCM online help.
- Use VCM's automated patch assessment and deployment to deploy patches. See "Deploying Patches with Automated Patch Assessment and Deployment" on page 169.

Enable the Trust and Patching Status for the Patching Repository Machine

You must enable the trust and patching repository status for the Red Hat Linux patching repository machine, to designate it as a trusted patching machine for security purposes.

You can use a single patching repository machine. The Red Hat Linux patching repository machine hosts the Software Content Repository (SCR) Tool that VCM uses to download patches from the vendor Web sites.

Prerequisites

- Set up a physical or virtual Red Hat Linux machine, running Red Hat version 6 or later, 64-bit, to be used for the Linux and UNIX patching repository. See the online Red Hat Customer Portal.
- (Optional) Set up one or more geographically distributed alternate location Red Hat Linux machines, running Red Hat 6, 64-bit. See the online Red Hat Customer Portal.

Procedure

1. In VCM on the VCM Collector, to set the repository status for the patching repository machine, click **Administration** and click **Certificates**.
2. (Optional) If the patching repository status is set for a different patching repository machine, disable the patching repository status to stop using that machine as the patching repository.
   a. In the Certificates data grid, click the existing Red Hat Linux machine that has the Patching Repository Status enabled.
   b. Click **Patching Repository**.
   c. Click **Disable**, click **Next**, and click **Finish**.
3. Enable the trust status for the Red Hat Linux machine that you are designating as the patching repository.
   a. In the Certificates data grid, click a single Red Hat Linux machine.
   b. Click **Change Trust Status**.
   c. Select the **Check to trust or uncheck to untrust the selected machines** check box and click **Next**.
4. Enable the patching repository status for the Red Hat Linux machine that you are designating as the patching repository.
   a. Click the Red Hat Linux machine.
   b. Click **Patching Repository**.
   c. Click **Enable**, click **Next**, and click **Finish**.

What to do next

Select a patching repository machine and an optional alternate location to store the Linux and UNIX patches. See "Configure How Managed Machines Stage Patches for Deployment" on page 165.

Configure How Managed Machines Stage Patches for Deployment

You must configure how the target managed machines obtain and stage the patches for VCM to deploy to the managed machines. VCM 5.7 supports staging patch files as large as 5GB.

For VCM to stage the Linux and UNIX patches and deploy them to managed machines, select a patching repository machine and an optional geographically distributed alternate location machine.

When a primary patching repository and one or more alternate location repositories are available, VCM copies the patches from the primary patching repository to either the target managed machines or to an alternate location machine for deployment to the target managed machines, depending on your selections. The target managed machines must be able to resolve the name of the alternate location machine that you type in the VCM Patch Staging wizard.

Prerequisites

- Configure the patching repository machine as a trusted machine and a patching repository. See "Enable the Trust and Patching Status for the Patching Repository Machine" on page 164.
- If you use credentials for patch staging, verify that the managed machine's certificate is trusted. See the VCM online help.
- Ensure you understand secure communication for patching. See the *VCM Security Guide*.

Procedure

1. In VCM, click **Administration**.
2. Click **Settings > General Settings > Patching > UNIX > Patch Staging**.
3. Click **Add**.
4. Type a unique name for the patching repository, type a description, and click **Next**.
5. Select the staging method for the Linux and UNIX managed machines to obtain the patch files for deployment, and click **Next**.

Option	Description
Obtain patches from the Patching Repository	During patch deployment, the target managed machines obtain the patches from the patching repository machine. The patching repository machine stores the patches that the Software Content Repository (SCR) Tool downloads from vendor Web sites.
Obtain patches from an Alternate Location	When you use one or more geographically distributed alternate Red Hat Linux machines to store the Linux and UNIX patches for deployment to managed machines, during the patch deployment the target managed machines obtain patches from the alternate location machine.

6. Select the patching repository machine from which VCM copies the patches.
   a. Type the path to the repository of Linux and UNIX patches on the patching repository machine.

      Depending on the protocol you use, you might need to use the relative path to the directory.

   b. Select a protocol to use when copying patches from the patching repository.

      This read operation uses HTTPS, HTTP, FTP, NFS, or a premounted file system. With a premounted file system, users can read and write files where appropriate. Permissions might require you to add the group that VCM uses to run the jobs on the managed machines.

   c. Select the port that the selected protocol uses to copy the patches from the patching repository.
   d. To require credentials to the patching repository, type the user name and password and click **Next** or **Finish**.
7. (Optional) If you selected **Obtain patches from an Alternate Location**, VCM copies the patches from the patching repository machine to a geographically distributed alternate location machine.

   During patch deployment, VCM copies the patches from the alternate location machine and stages them on the target managed machines for deployment.

   a. Type the host name or IP address of the alternate location machine.
   b. Type the path to the directory used to store the patches.
   c. Select the protocol used to copy the patches from the patching repository machine to the alternate location machine.

      This write operation uses FTP, NFS, or File, a premounted file system.

   d. Select the port used by the selected protocol to copy the patches.
   e. To require credentials to copy the patches, type the user name and password and click **Next**.

8. (Optional) If you selected **Obtain patches from an Alternate Location**, you must provide the path and connection information to copy the patches from the alternate location machine to the target managed machines.
   a. (Optional) If necessary, change the path where the patches reside.

      VCM populates this path from the previous screen to match it to the patching repository file structure.

   b. Select the protocol used to copy patches from the alternate location machine to the target managed machines.

      This read operation uses HTTPS, HTTP, FTP, NFS, or File, a premounted file system.

   c. Select the port that the selected protocol uses to copy the patches.

   d. To require credentials to copy the patches, type the user name and password and click **Finish**.

What to do next

Configure the machine group mapping for VCM to use to patch the target managed machines. See "Configure the Machine Group Mapping to Use the Patch Staging Configuration" on page 167.

Configure the Machine Group Mapping to Use the Patch Staging Configuration

You must configure the machine group for VCM to use to deploy Linux and UNIX patches to target managed machines. You can combine Linux and UNIX managed machines into a single machine group, and have VCM use a single action to deploy the patches to all of the managed machines in that group.

VCM uses the alternate location defined in the machine group mapping to deploy patches to the managed machines. During the patch deployment, VCM stages the Linux and UNIX patches from the patching repository or the optional alternate location machine to the target managed machines, then deploys the patches to those machines.

By default, VCM stages the patches in the `/tmp` directory on the managed machines. However, vendors such as HP, Oracle, and IBM, can bundle multiple patches into a set, and the `/var/tmp` directory is used to process the patches during patch deployment.

Prerequisites

- Configure how the target managed machines obtain and stage the patches for VCM to deploy to the managed machines. See "Configure How Managed Machines Stage Patches for Deployment" on page 165.
- Verify that the machine groups for VCM to use during the patch deployment are defined. If machine groups are not available to patch your specific groups of managed machines, you must add them. See the VCM online help.

Procedure

1. Click **Administration** and select **Settings > General Settings > Patching > Machine Group Mapping**.
2. Select a machine group and click **Edit**.
3. Select a deployment type.

Option	Description
Standard Deployment	VCM deploys the Linux and UNIX patches from a standard predefined patch directory, such as `/tmp`, on the target managed machines. The standard path for deployment is defined in UNIX Additional Settings.
Custom Deployment	VCM deploys the Linux and UNIX patches from a custom patch directory on the target managed machines. You must type the path to the directory where the patches reside on the target managed machines.

4. Select a source for the patches for VCM to use to stage the patches on the target managed machines during patch deployment.

   The source can be the patching repository machine, a geographically distributed alternate location machine, or None. If you select None, you must manually stage the patches on the target managed machines.

5. Select the type of temporary path to use on the target managed machines for VCM to extract the Linux and UNIX patches and temporary files.

Option	Description
Standard Temp Path	VCM deploys Linux and UNIX patches from a standard predefined patch directory on the target managed machines, such as `/var/tmp`. The standard path is defined in UNIX Additional Settings for the setting named Default Machine Group Mapping location for patch deployments.
Custom Temp Path	VCM deploys Linux and UNIX patches from a custom path. You must type the custom path in the text box. The custom path is defined in UNIX Additional Settings for the setting named Default Machine Group Mapping for temporary files during patch deployment.

6. Type the path to the temporary files on the managed machines and click **Next**
7. Review the settings and click **Finish**.

What to do next

- Verify that the Software Content Repository (SCR) Tool base path in VCM points to the location where you installed the SCR Tool on the patching repository machine. See "Verify the SCR Tool Base Path for the Patching Repository" on page 168.
- Use VCM to deploy the patches to target Linux and UNIX managed machines. See "Deploying Patches with Automated Patch Assessment and Deployment" on page 169.

Verify the SCR Tool Base Path for the Patching Repository

The setting for the Software Content Repository (SCR) Tool base path in VCM must point to the location where you installed the SCR Tool on the patching repository machine.

The base path directory contains directories for the SCR Tool binary files, configuration files, logs.

Prerequisites

Configure the machine group mapping for VCM to use to patch the target managed machines. See "Configure the Machine Group Mapping to Use the Patch Staging Configuration" on page 167.

Procedure

1. In VCM, click **Administration**.
2. Select **Settings > General Settings > Patching > UNIX > Additional Settings**.
3. Verify that the value for the **Default UNIX/Linux package repository SCR base path** setting value is the location on the patching repository machine where you installed the SCR Tool, such as `/SCR`.
4. Verify that the value for the **Default UNIX/Linux package repository path** setting value is the location used in the Red Hat properties file properties file, such as *`/var/www/html/vendorfiles`*.

   For example, `# mkdir /var/www/html/vendorfiles /SCR/cacherequest`.

What to do next

Deploy patches to managed machines. See "Deploying Patches with Automated Patch Assessment and Deployment" on page 169.

Deploying Patches with Automated Patch Assessment and Deployment

VCM supports automatic, event-driven and scheduled patch deployment in distributed environments for Linux, UNIX, and Windows patching. Automatic patching helps you stage and deploy patches with ease to ensure that your managed machines always receive the current updates. When certain events occur, VCM triggers an automatic patch deployment.

When any of the following events occur, VCM deploys the patches in the patch assessment templates associated with a machine group, with any exceptions applied to the machine group and the assessment results of the template. The exception is applied to the assessment results, and the machines are exempted from the patch deployment.

- New downloaded patch content matches the filter used in a dynamic patching assessment template, or you edit the template to change the bulletins included in it. VCM updates the bulletin membership in the patching assessment template and triggers an automatic patch deployment. If the template is assessed after a collection, the change in patch applicability triggers an automatic patch deployment.
- You add a machine to a machine group and the membership is updated for any machine group that is associated with an automatic deployment. VCM begins the automatic patch deployment, and the results are updated for static or dynamic patching templates.
- You collect the patch status from managed machines, and run a patch assessment on those machines. If the machines are part of the machine group that is mapped to an assessment template in the automatic deployment wizard, VCM determines which managed machines require patches and begins the automatic patch deployment.
- You scheduled VCM to run an automatic patch deployment later, and collected patch data or scheduled the patch data collection after you created the automatic deployment but before the scheduled time to run the automatic deployment. VCM begins the automatic patch deployment at the scheduled time.

During event-driven patch deployment, managed machines obtain the patches from the patching repository machine or from an alternate location machine. If you use one or more alternate location machines to store the Linux and UNIX patches for deployment to managed machines, the managed machines obtain the patches from the alternate location machine during the patch deployment.

You can also use VCM's automatic event-driven and scheduled patching for managed Windows machines. For a list of supported machines for VCM patching, see the *VCM Installation Guide*.

To configure VCM for automatic, event-driven patch deployment, see "Configure VCM for Automatic Event-Driven Patch Assessment and Deployment" on page 170.

To configure VCM for automatic scheduled patch deployment, see "Configure VCM for Automatic Scheduled Patch Assessment and Deployment" on page 176.

To manually deploy patches to managed machines, see the VCM online help.

Configure VCM for Automatic Event-Driven Patch Assessment and Deployment

To ensure that Linux, UNIX, and Windows managed machines always include the latest patches, you can have VCM deploy patches to the managed machines when certain events occur in your environment. After you perform the initial configuration for the automatic deployment, no intervention is required to deploy patches to managed machines.

To configure the automatic, event-driven patch assessment and deployment, you must generate a patch assessment template and run a patch assessment on the managed machines. Optionally, you can add exceptions for the automatic patch deployment.

To support automated patching of Linux and UNIX managed machines, VCM uses a job chain. The steps in the job chain download patches from vendor sites to the patching repository, copy the patches to the alternate location machines, stage patches on the target Linux and UNIX managed machines, deploy the patches to managed machines, and reboot the managed machines. The status of the job chain, including the running jobs in the job chain, appears in the VCM Job Manager. Finished job chain jobs appear in Job Manager History.

VCM supports patching exceptions for machines that should not be patched using VCM, and for specific patches or bulletins that VCM should not deploy. VCM also supports exceptions for specific patches or bulletins that do not apply to certain machine groups, or patches or bulletins that are not necessary, because they are already deployed. VCM applies patching exceptions during the automatic patch deployment process to the machine group that you select when you define the automatic deployment mapping.

When VCM deploys patches to managed machines, a job is created for each machine. When a reboot of the managed machine is required, VCM creates a deployment job and a reboot job for the machine. The deployment occurs either immediately or when scheduled. After the deployment is finished, the reboot job begins either immediately or at the scheduled time. If the scheduled time has passed, the reboot job fails.

Depending on the number of managed machines being patched and the number of jobs, the time allowed for the patching window might expire before the patching jobs are finished, because the request might become stale or the number of maximum concurrent VCM Agent installations might be set too low. If patching jobs time out, see the troubleshooting topic in the *VCM Troubleshooting Guide*.

Prerequisites

Configure VCM. See "Configuring VCM to Work with the Patching Repository and Alternate Locations" on page 162.

Procedure

1. "Generate a Patch Assessment Template" on page 171

   To configure VCM for automatic, event-driven patch deployment, you must generate a patch assessment template to use with the automatic patch deployment mapping.

2. "Run a Patch Assessment on Managed Machines" on page 172

   You must run the patch assessment template to collect patch status data from the managed machines.

3. "Add Exceptions for Patching Managed Machines" on page 172

   You can optionally add patching exceptions for the automatic patch deployment.

4. "Configure the VCM Administration Settings" on page 173

   VCM provides settings for automatic patch deployment, including template and group membership, patch applicability, and default threshold data age. You can set the default repository host, repository path, and Software Content Repository (SCR) Tool base path settings.

5. "Generate a Patch Deployment Mapping" on page 175

   VCM provides settings for automatic patch deployment, including template and group membership, patch applicability, and default threshold data age. You can set the default repository host, repository path, and Software Content Repository (SCR) Tool base path settings.

What to do next

- For Linux and UNIX patching, after a job triggers, view the job chain in the VCM Job Manager, and finished job chain jobs in Job Manager History. See "How the Linux and UNIX Patching Job Chain Works" on page 178.
- (Optional) You can schedule an automatic patch deployment. When you schedule VCM to run an automatic patch deployment later, and collected patch data or scheduled the patch data collection after you created the automatic deployment but before the scheduled time to run the automatic deployment. VCM begins the automatic patch deployment at the scheduled time. See "Configure VCM for Automatic Scheduled Patch Assessment and Deployment" on page 176.

Generate a Patch Assessment Template

To configure VCM for automatic, event-driven patch deployment, you must generate a patch assessment template to use with the automatic patch deployment mapping. VCM uses the patch assessment template to collect patch assessment data from Linux, UNIX, or Windows managed machines in your environment.

With automatic, event-driven patch deployment, you configure a patch assessment template with a machine group, and VCM deploys patches to the Linux, UNIX, or Windows patching assessment template that you associate with the machine group.

To create a dynamic membership of bulletins for the Linux and UNIX patch assessment, you can use dynamic patching assessment templates to apply filter criteria. After new patch content is available, VCM updates the bulletin membership of a dynamic assessment template. To exclude certain patches from being applied to a specific set of managed machines or from all managed machines in your environment, you can create patching exceptions for dynamic and static patching assessment templates.

Prerequisites

Review the steps to configure the automatic, event-driven patch assessment and deployment. See "Configure VCM for Automatic Event-Driven Patch Assessment and Deployment" on page 170.

Procedure

1. To generate a static or dynamic patch assessment template and include the relevant patch bulletins, click **Patching** and select **All UNIX/Linux Platforms > Assessment Templates**.
2. Click **Add** to add a patch assessment template.
   a. To add a static patch assessment template, add available patch bulletins to the template.
   b. To add a dynamic patch assessment template, define a filter with one or more filter rules.

      For example, you can select the patch architecture, bulletin number, severity, and so on.
3. Click **Finish** to save the patch assessment template.

What to do next

Run the patch assessment template. See "Run a Patch Assessment on Managed Machines" on page 172.

Run a Patch Assessment on Managed Machines

You must run the patch assessment template to collect patch status data from the managed machines.

Prerequisites

Generate the patch assessment template. See "Generate a Patch Assessment Template" on page 171.

Procedure

1. To use the patch assessment template you created to run a patch assessment on the managed machines, click **Patching**.
2. Select **All UNIX/Linux Platforms > Assessment Templates**.
3. Click the patch assessment template that you added.
4. Click **Assess**.
5. Select filters and select the Patch Assessment Data Class default filter to collect all patch assessment results.
6. Click **Finish** to begin the patch assessment.

What to do next

Add exceptions. See "Add Exceptions for Patching Managed Machines" on page 172.

Add Exceptions for Patching Managed Machines

You can optionally add patching exceptions for the automatic patch deployment.

VCM supports patching exceptions for machines that should not be patched using VCM, and for specific patches or bulletins that VCM should not deploy. VCM also supports exceptions for specific patches or bulletins that do not apply to certain machine groups, or patches or bulletins that are not necessary, because they are already deployed.

VCM applies patching exceptions during the automatic patch deployment process to the machine group that you select when you define the automatic deployment mapping.

The following procedure is optional.

Prerequisites

Run a patch assessment. See "Run a Patch Assessment on Managed Machines" on page 172.

Procedure

1. To add patching exceptions for VCM to apply during the automatic deployment of patches to a group of managed machines, click **Patching**.
2. Select **All UNIX/Linux Platforms > Exceptions**.
3. Click **Add** and name the patching exception.
4. Select the machine group to which the patching exception applies.
5. Set the patching exception override options and expiration date.
6. Add one or more rules for the patch exception.

   For example, you can add patching exceptions rules for the operating system, data age, patch status, severity, and so on.
7. Click **Finish** to save the patching exception.

What to do next

Configure the VCM Administration settings. See "Configure the VCM Administration Settings" on page 173.

Configure the VCM Administration Settings

VCM provides settings for automatic patch deployment, including template and group membership, patch applicability, and default threshold data age. You can set the default repository host, repository path, and Software Content Repository (SCR) Tool base path settings. With the VCM administration settings for patching, you can also match patch content downloads with platforms, set the machine group mapping.

Prerequisites

- (Optional) Add patching exceptions. See "Add Exceptions for Patching Managed Machines" on page 172.
- If you must enter sensitive parameters for patching with VCM, to enable VCM to use an HTTPS bypass to allow HTTP communication, set the HTTPS bypass in the VCM Collector settings in **Administration > Settings > General Settings > Collector**.

Procedure

1. To modify the automatic patching settings, click **Administration**.
2. Click **Settings > General Settings > Patching > UNIX > Additional Settings**.
3. According to your patch assessment and deployment strategy, click **Edit Setting** for each of the automatic patch deployment settings, then modify and save the setting.

Option	Description
Automatic patch deployment-Automatically deploy patches whenever membership of associated machine groups changes	VCM deploys patches when you add a machine to a machine group and the membership is updated for any machine group that is associated with an automatic deployment. VCM begins the automatic patch deployment, and the results are updated for static or dynamic patching templates.
Automatic patch deployment-Automatically deploy patches whenever membership of associated templates changes	VCM deploys patches when new downloaded patch content matches the filter used in a dynamic patching assessment template, or you edit the template to change the bulletins included in it. VCM updates the bulletin membership in the patch assessment template and triggers an automatic patch deployment.
Automatic patch deployment-Automatically deploy patches whenever patch applicability changes	VCM deploys patches when you collect the patch status from managed machines, and run a patch assessment on those machines. If the machines are part of the machine group that is mapped to an assessment template in the automatic deployment wizard, VCM determines which managed machines require patches and begins the automatic patch deployment. If the template is assessed after a collection, the change in patch applicability triggers an automatic patch deployment.
Automatic patch deployment-Default threshold data age (days)	Sets the patching data age threshold, in days, for the collected patch data, which defines how old the collected patch data can be before VCM deploys the patches. When the data age of the bulletin is greater than the threshold data age, VCM does not deploy the patches. You must run a new collection and assessment to update the data age for the patch bulletin.

4. Review the additional patching settings, and make any changes required for your environment.
   a. Set the patching content download to match the licensed platform types.
   b. Set the default machine group mapping path for temporary files during patch deployment.
   c. Set the default machine group mapping location for patch deployments.
   d. Set the default Linux and UNIX repository host, path, and SCR base path.
   e. Define the platforms for which patching content is downloaded and parsed.

What to do next

- Generate a patch deployment mapping. See "Generate a Patch Deployment Mapping" on page 175.
- (Optional) You can schedule an automatic patch deployment. When you schedule VCM to run an automatic patch deployment later, and collected patch data or scheduled the patch data collection after you created the automatic deployment but before the scheduled time to run the automatic deployment. VCM begins the automatic patch deployment at the scheduled time. See "Configure VCM for Automatic Scheduled Patch Assessment and Deployment" on page 176.

Generate a Patch Deployment Mapping

To have VCM deploy patches to managed machines when the configured events occur, you must define an automatic patch deployment mapping. When any of the trigger conditions occur, VCM deploys the designated patches to the managed machines.

After the automatic patch deployment job is finished, VCM performs another patch assessment on the managed machines to report the updated patch status for the managed machines.

To generate an automatic patch deployment mapping of a Linux or UNIX machine group, you select the patch assessment template to apply to the machine group.

The following procedure is for Linux and UNIX machines, but you can also use VCM's automatic event-driven and scheduled patching for supported Windows machines.

Prerequisites

Configure the VCM Administration settings. See "Configure the VCM Administration Settings" on page 173.

Procedure

1. Click **Patching** and select **All UNIX/Linux Platforms > Automatic Deployment**.
2. To add an automatic deployment mapping, click **Add**, type a name and description for the mapping, and click **Next**.
3. Click the machine group to use for the automatic scheduled patch deployment.
4. Click the patching assessment template that you created, and click **Next**.
5. Select the **Event-Driven Automatic Deployment Run** for the type of automatic deployment.
6. Select an automatic deployment reboot option.
7. Type a number for the threshold data age and click **Next**.

   The threshold data age indicates the number of days allowed since the last patch assessment was run on the managed machine, before VCM can run the automatic patch deployment on the managed machine.
8. Define the schedule to run the automatic patch deployment, including how often the automatic scheduled patching occurs, the time of day, and the start and end dates, and click **Next**.
9. Review the summary and click **Finish** to schedule the automatic patch deployment.

What to do next

- After VCM triggers a patch assessment, view the patch assessment results. See the VCM online help.
- (Optional) You can schedule an automatic patch deployment. When you schedule VCM to run an automatic patch deployment later, and collected patch data or scheduled the patch data collection after you created the automatic deployment but before the scheduled time to run the automatic deployment. VCM begins the automatic patch deployment at the scheduled time. See "Configure VCM for Automatic Scheduled Patch Assessment and Deployment" on page 176.

Configure VCM for Automatic Scheduled Patch Assessment and Deployment

To ensure that Linux, UNIX, and Windows managed machines are updated with the latest patches on a regular basis, you can schedule VCM to deploy patches to the managed machines. The automatic scheduled patch assessment and deployment matches a machine group to a patch assessment template.

To configure the automatic scheduled patch assessment and deployment, you must generate a patch assessment template. Optionally, you can add exceptions for the automatic patch deployment.

Prerequisites

Configure VCM. See "Configuring VCM to Work with the Patching Repository and Alternate Locations" on page 162.

Procedure

1. Click **Patching** and select **All UNIX/Linux Platforms > Automatic Deployment**.
2. To add an automatic deployment mapping, click **Add**, type a name and description for the mapping, and click **Next**.
3. Click the Linux, UNIX, or Windows machine group to use for the automatic scheduled patch deployment.
4. Click the patching assessment template that you created, and click **Next**.
5. Select the **Scheduled Automatic Deployment Run** for the type of automatic deployment run option.
6. Select an automatic deployment reboot option.
7. Type a number for the threshold data age and click **Next**.

   The threshold data age indicates the number of days allowed since the last patch assessment was run on the managed machine, before VCM can run the automatic patch deployment on the managed machine.
8. Define the schedule to run the automatic patch deployment, including how often the automatic patching occurs, the time of day, and the start and end dates, and click **Next**.
9. Review the summary and click **Finish** to schedule the automatic patch deployment.

What to do next

- For Linux and UNIX patching, after a job triggers, view the job chain in the VCM Job Manager, and finished job chain jobs in Job Manager History. See "How the Linux and UNIX Patching Job Chain Works" on page 178.

How the Linux and UNIX Patch Staging Works

As a patch administrator, you can stage patches on target Linux and UNIX managed machines for VCM to deploy. With patch staging, the patches are available in a directory on the target managed machines in preparation for deployment.

Target managed machines copy the patches from either the patching repository machine or an alternate location machine. After the patches are stored in the patch repository or on the alternate location machines, during the patch deployment you can schedule the patch staging to target managed machines before the deployment occurs. You can have VCM deploy the patches immediately after you stage them or when certain conditions occur, which trigger an automatic patch deployment.

With the patch deployment schedule, you can stage the patches on the target managed machines immediately or at a later time before the scheduled deployment occurs. Otherwise, you must manually stage the patches on the target managed machines.

When you set up a patching repository machine and alternate location machines, you must ensure that users have proper permissions and protocols configured to read patches from the patching repository machine and write patches to the alternate location machines.

VCM staging of Linux and UNIX patches performs the following actions.

- The patching repository machine retrieves Linux and UNIX patches from the vendor Web sites and stores them in its local patch repository.
- To make the patches available for deployment to target managed machines, VCM copies the patches from the patching repository to the alternate locations, or to the target managed machines, depending on whether you have alternate location machines in your patching environment.

Option	Description
Copy patches from the patching repository	Target managed machines copy patches from the patching repository to stage the patches for deployment.
Copy patches from an alternate location	In a geographically distributed patching environment, VCM copies patches from the patching repository machine to an alternate location machine to stage the patches on the target managed machines for deployment. ■ VCM uses FTP, NFS, or File, a premounted file system, to copy the patches to the alternate location machine. ■ VCM uses HTTP, HTTPS, FTP, NFS, or File, a premounted file system, to copy the patches from an alternate location to the target managed machines.

- In the patch deployment action, VCM stages the patches in the standard or custom patch directory on the target Linux and UNIX managed machines. Then VCM deploys the patches immediately or at the time that you schedule the patch deployment in the Deploy wizard.

After VCM finishes the patch deployment, you can run another patch assessment to verify that the patches are applied to the managed machines.

Related Topics

- For steps to stage Linux and UNIX patches for deployment, see "Configuring VCM to Work with the Patching Repository and Alternate Locations" on page 162 and "Configure How Managed Machines Stage Patches for Deployment" on page 165.
- For a description of events that VCM uses to trigger an automatic patch deployment, see "Configure VCM for Automatic Event-Driven Patch Assessment and Deployment" on page 170.

How the Linux and UNIX Patching Job Chain Works

The VCM job chain is a set of job steps used to automate the patching flow for Linux and UNIX managed machines. The job chain includes the following steps.

1. Download Linux and UNIX patches from OS vendor sites, such as Red Hat, SUSE, and so on, and store them in the patching repository.
2. Copy the patches from the primary patching repository machine to a geographically distributed alternate location machine.
3. Stage the patches on the Linux and UNIX target managed machines to be patched.
4. Deploy the patches to the target managed machines.
5. (Optional) Reboot the target managed machines.

When a Linux or UNIX patching job requires only the patch deployment step and an optional reboot of the managed machines, VCM does not use a job chain.

VCM displays the state of the running job chain jobs in the Patching Job Manager and the Administration Job Manager, with the job steps and actions in the chain. Finished jobs appear in the job history.

After VCM begins the patching job and the job chain steps, you cannot alter the job chain.

- In the VCM Patching Job Manager or Administration Job Manager, when a job chain is running for scheduled and pending jobs, you cannot edit or disable the job chain, but you can delete it. To cancel a job chain, you must use the VCM Administration Job Manager. When you cancel a job in the job chain, VCM cancels the entire job chain.
- In the VCM Patching Job Manager or Administration Job Manager, when a job chain appears in the Running or Scheduled node, you can cancel the job chain if you select any link in the job chain. Canceling any part of a chain cancels the entire job. You cannot rescheduled the job chain.

How the Deploy Action Works

The patch deployment action runs a command from the VCM Collector to the managed machines.

The VCM job command performs the following actions.

- Assesses VCM managed machines to determine whether the patch was installed since the last assessment.
- Runs a preinstall script as a remote command, if specified.
- Installs the patch that already resides on the VCM managed machine's mounted or local file system.
- Runs a postinstall script as a remote command, if specified.
- Assesses whether the patch was installed on the VCM managed machine.

The preinstall and postinstall scripts used in the deployment actions are remote commands, which differ from using a VCM remote command to install a patch.

The patch assessment and deployment process for Linux and UNIX does not use remote commands. If you deploy a patch using a user-created remote command, the patch is not assessed until you run another assessment.

When VCM deploys patches to managed machines, a job is created for each machine. When a reboot of the managed machine is required, VCM creates a deployment job and a reboot job for the machine. The deployment occurs either immediately or when scheduled. After the deployment is finished, the reboot job begins either immediately or at the scheduled time. If the scheduled time has passed, the reboot job fails.

Depending on the number of managed machines being patched and the number of jobs, the time allowed for the patching window might expire before the patching jobs are finished, because the request might become stale or the number of maximum concurrent VCM Agent installations might be set too low. If patching jobs time out, see the troubleshooting topic in the *VCM Troubleshooting Guide*.

Patch Deployment Wizards

To have VCM deploy patches to Linux, UNIX, and Windows managed machines, use the patch deployment wizards or use the automatic patch deployment feature.

- Linux and UNIX Patching Deploy Wizard
- Windows Patching Deploy Wizard

Deploying patches to Linux, UNIX, or Windows managed machines requires that you create a patch assessment template and assess the patch state of managed machines.

- To assess the patch state of Linux and UNIX managed machines, collect patch assessment data, create the patch assessment template, run the patch assessment on managed machines, explore the patch assessment results, and deploy patches to the managed machines.
- Before you assess the patch state of Windows managed machines, use the VCM patching filter sets to collect patch data from managed machines. Then create the patch assessment template, run the patch assessment, explore the patch assessment results, and deploy patches to the managed machines.

To deploy patches on Linux and UNIX managed machines, use the Deploy wizard in one of the following Patchinglocations.

- User-created patching assessment templates
- Imported patching assessment templates
- Assessment results for all bulletins

To deploy patches on Windows managed machines, use the Deploy wizard in one of the following Patchinglocations.

- User-created patching assessment templates
- Imported patching assessment templates

An imported template is a text file patch deployment utility that contains one or more managed machines, patches, or combinations of managed machines and patches. You can include command-line options in imported templates for Linux and UNIX machines.

CAUTION VMware does not translate or validate any command-line options used during patch deployment.

Running Patching Reports

VCM uses trends, details, template summaries, bulletins, affected software products, and patch deployment history to generate patch status reports for Linux, UNIX, and Windows managed machines.

With real-time patch assessment reports, you can generate SQL reports for managed machines that are assessed against bulletins and affected software products. You can report on the history of patch deployments using the patch assessment results.

You can generate the following report types.

- Real-time assessment reports by bulletins or products
- Real-time assessment reports by affected software products
- Real-time assessment reports of bulletins and products
- Patch deployment history reports

When you generate reports, you can take the following actions.

- Manually update VCM patching Windows content.
- Run reports when VCM does not have access to the Internet.

10 Running and Enforcing Compliance

Compliance compares your virtual or physical machines running Linux, UNIX, Mac OS X, or Windows operating systems against configuration standards that you download, or that you create, to determine if the machines meet the standards. The results of the compliance run notify you which machines meet configuration settings meet the standards and which ones do not meet the standards. In some cases, you can enforce certain settings on the machines that are not in compliance, initiating the changes from VCM.

Preset rules and templates are available that enable you to begin monitoring system compliance to regulatory (Sarbanes-Oxley, HIPAA, GLBA and FISMA) industry and Microsoft standards. You can create and manage rules and rule groups based on Active Directory (AD) objects and configuration data, or on machine data.

IMPORTANT Compliance does not query individual systems; it only queries the database. If a machine has not been included in a Collection, or the necessary information has not been included in a Collection, or the last Collection is outdated, the Compliance Monitor will measure incorrect or out-of-date data. Therefore, for accurate Compliance monitoring, you must first collect the necessary data.

Running Machine Group Compliance

Compliance templates evaluate the data collected from virtual or physical machines in machine groups to determine if the machines meet the rules in the templates. If the property values on a machine do not meet the rule criteria, and if no exception is defined, then the machine is flagged as noncompliant. When a machine is noncompliant, the template results provide the details of the settings or configurations that do not match the rules. You can use this information to resolve the problem.

Compliance templates include the following components:

- **Rule Groups:** A rule group comprises rules and filters.
- **Rules:** The rules define the optimal configuration standards.
- **Filters:** The filters limit the machines on which the template runs to only the machines that meet the filter criteria. If filters are not defined, the rules are run against all machines in the machine group based on the data types against which the rules run.
- **Exceptions:** The exceptions are optional permanent or temporary exceptions to the template results. The defined exception indicates that a specific result is compliant or noncompliant, even though it does not match the requirements of the rules.

After you configure your compliance templates, you can optimize how VCM monitors the compliance of machines in your environment using alerts and scheduling regular compliance template runs on your collected machine group data.

To assist you with managing your environment, you can download compliance templates from the VMware Center for Policy and Compliance. The available templates include, for example, SOX, HIPAA, PCI DSS, and VMware vSphere hardening and other regulatory compliance templates.

Download and Import Compliance Content

You can use the Content Wizard Tool to download and install selected compliance templates directly to theVCM database.

VMware provides predefined templates that you can download from the Center for Policy and Compliance. Some of the available templates include SOX, HIPAA, PCI DSS, and VMware vSphere templates that are based on hardening guides and published industry security standards. After downloading and installing the templates, you can run them as provided or modify them to meet the needs of your environment.

The VMware vSphere 5.0 Security Hardening Guide is used as the example compliance content.

Prerequisites

- Install the Content Wizard Tool. The tool is installed on the Collector if you performed a default installation.
- Verify that the Windows machine on which you are running the Content Wizard Tool has Internet access.
- Ensure that you configured the system requirements for your environment. See Content Wizard Tool System Configurations in the tool online Help.
- Configure the settings for your environment. See Settings Menu in the tool online Help.
- Verity that you have the required permissions to import data to the VCM database. See Verify the VCM User Permissions in the tool online Help.

Procedure

1. On the Collector, click **Start** and select **All Programs > VMware vCenter Configuration Manager > Tools > Content Wizard Tool**.
2. Click **Get Updates from the Internet** and click **Next**.
3. After the updates are identified, click **Next**.
4. Select the updates to install and double-click**Install**.

   For example, VMware vCenter Configuration Manager Hardening guide.
5. When the import process is finished, review the Event Log Results to verify a successful download and click**Close**.
6. In the Content Wizard, click **Exit**.

What to do next

In VCM, locate the downloaded templates. For example, VMware vCenter Configuration Manager Hardening guide is in the Compliance slider, under Machine Group Compliance Templates. You can run the associated collection filter and then run the templates as delivered, or modify them to suit the requirements of your environment.

Create and Run Machine Group Compliance Templates

The compliance templates evaluate your machine group data to determine if the machines meet the criteria in the rules that define machines as compliant or noncompliant.

You can create your own compliance templates or modify templates that you downloaded from the Center for Policy and Compliance.

Prerequisites

- Collect data from your virtual and physical machines for the data types against which your compliance templates and filter sets run. See "Collect Linux, UNIX, and Mac OS X Data" on page 132 and "Collect Windows Data" on page 93.
- Download existing compliance templates that are applicable to your environment from the VMware Center for Policy and Compliance. See "Download and Import Compliance Content" on page 182.

Procedure

1. "Create Machine Group Compliance Rule Groups" on page 183

   Rule groups contain compliance rules and filters. You must create rule groups that you then assign to compliance templates.

2. "Create and Test Static Machine Group Compliance Rules" on page 184

   You create rules that define the ideal values that virtual or physical machines should have to be considered compliant.

3. "Create and Test Machine Group Compliance Filters" on page 185

   You can create filters that limit the virtual or physical machines on which the templates run to only the machines that meet the filter criteria.

4. "Preview Machine Group Compliance Rule Groups" on page 186

   You use the rules preview action, with the filters turned off and then turned on, to determine if a rule group is returning the expected results.

5. "Create Machine Group Compliance Templates" on page 187

   You can create compliance templates that include one or more rule groups that assess your selected virtual or physical machine group to determine which machines are compliant and noncompliant.

6. "Run Machine Group Compliance Templates" on page 188

   You run templates against your collected data to determine which virtual or physical machines are compliant or noncompliant.

7. "Resolve Noncompliant Compliance Template Results" on page 189

   The results for the compliance templates indicate whether the virtual or physical machine are compliant or noncompliant. If the machine is noncompliant, you can enforce noncompliant results manually or using VCM, or you can add an exception for expected noncompliant results.

8. "Configure Alerts and Schedule Machine Group Compliance Runs" on page 192

   (Optional) To optimize how VCM monitors the compliance of physical and virtual machines in your environment, configure alerts and schedule regular compliance template runs on your collected machine group data.

Create Machine Group Compliance Rule Groups

Rule groups contain compliance rules and filters. You must create rule groups that you then assign to compliance templates.

Templates can include one or more rule groups. Rule groups comprise rules and filters.

The collection filter set that is selected is used when calculating data age for the rules in the compliance templates. The filter set must collect the same data types that are included in the rules in the rule group. If the filter set does not collect the same data types, no data age is calculated.

This procedure demonstrates how to check whether your Linux machines, except those running 64-bit operating systems, have at least a 5GB hard drive capacity.

Procedure

1. Click **Compliance**.
2. Select **Machine Group Compliance > Rule Groups**.
3. Click **Add**.
4. Type the rule group name and description in the text boxes.

   In this example, Capacity 5GB - Linux and UNIX.
5. Select the Filter Set in the drop-down menu and click **OK**.

What to do next

Add a rule to the rule group. See "Create and Test Static Machine Group Compliance Rules" on page 184.

Create and Test Static Machine Group Compliance Rules

You create rules that define the ideal values that virtual or physical machines should have to be considered compliant.

A dynamic rule is based on a model machine. As the model machine changes, the required values change with it. A static rule is based on a value that you define.

This procedure demonstrates how to check whether your Linux machines, except those running 64-bit operating systems, have at least a 5GB hard drive capacity.

Prerequisites

- Create a rule group. See "Create Machine Group Compliance Rule Groups" on page 183.
- If you are creating rules based on software provisioning data as either a check or a remediation action, see "Create Compliance Rules Based on Software Provisioning Data" on page 230 or "Create Compliance Rules Containing Software Provisioning Remediation Actions" on page 231.

Procedure

1. Click **Compliance**.
2. Select **Machine Group Compliance > Rule Groups > rule group name > Rules**.
3. Click **Add**.
4. Type the name and description in the text boxes and click **Next**.

   For example, Linux and UNIX Disk Cap > 5 GB.
5. Expand **Linux**, select **Disk Info - Hard Drive**, and click **Next**.
6. Select **Basic** and click **Next**.
7. Click **Add** and configure the rules with the ideal values.
   a. In the properties drop-down menu, select **Total Capacity (MB)**.
   b. Select **>** as the rule operator.
   c. Click the ellipsis button or type **5120**, and click **OK**.
   d. Click **Next**.
8. Select the **Severity** of a failure in the drop-down menu and click **Next**.
9. Review the changes and click **Finish**.

   The rule is added to the data grid.
10. Select your new rule and click **Preview**.
11. Select **Do not apply machine filters to preview** and click **OK**.

    When you test a rule, first test without the filter to ensure that the rule returns the expected results.
12. Review the data in the **Non-compliant results** window to verify that your rule is behaving as expected.

What to do next

Add a filter to the rule group. See "Create and Test Machine Group Compliance Filters" on page 185.

Create and Test Machine Group Compliance Filters

You can create filters that limit the virtual or physical machines on which the templates run to only the machines that meet the filter criteria.If filters are not defined, the rules are run against all virtual or physical machines in the selected machine group group.

This procedure demonstrates how to check whether your Linux machines, except those running 64-bit operating systems, have at least a 5GB hard drive capacity.

Prerequisites

- Create a rule group. See "Create Machine Group Compliance Rule Groups" on page 183.
- Create a rule. See "Create and Test Static Machine Group Compliance Rules" on page 184.

Procedure

1. Click **Compliance**.
2. Select **Machine Group > Rule Groups > rule group name > Filters**.
3. Click **Add**.
4. Type the name and description in the text boxes and click **Next**.

   For example, Architecture not x86_64.
5. Expand **Linux**, select **Machines - General**, and click **Next**.

   The collected data for this data type includes machine architecture.
6. Select **Basic** and click **Next**.
7. Click **Add** and configure the filter with the values to limit assessed machines or to exclude machines from assessment.
   - In the properties drop-down menu, select **Machine Architecture**.
   - Select <> as the filter operator.
   - Click the ellipsis, select **x86_64**, and click **OK**.
   - Click **Next**.
8. Review the changes and click **Finish**.

   The filter is added to the data grid.
9. Select your new filter and click **Preview**.
10. Review the data in the Machines window to verify that your filter is behaving as expected.

What to do next

Test your rule and filter together. See "Preview Machine Group Compliance Rule Groups" on page 186.

Preview Machine Group Compliance Rule Groups

You use the rules preview action, with the filters turned off and then turned on, to determine if a rule group is returning the expected results.

This procedure demonstrates how to check whether your Linux machines, except those running 64-bit operating systems, have at least a 5GB hard drive capacity.

Prerequisites

- Create a rule group. See "Create Machine Group Compliance Rule Groups" on page 183.
- Create a rule. See "Create and Test Static Machine Group Compliance Rules" on page 184.
- Create compliance filters. See "Create and Test Machine Group Compliance Filters" on page 185.

Procedure

1. Click **Compliance**.
2. Select **Machine Group Compliance > Rule Groups**.

   Capacity 5GB - Linux and UNIX is the example in this procedure.
3. Select your new rule group and click **Preview**.
4. Select **Do not apply machine filters to preview** and click **OK**.

   When you test a rule, test first without the filter to ensure that the rule returns the expected results.
5. Review the data in the **Non-compliant results** window to verify that your rule is behaving as expected.
6. Close the window.
7. Select your new rule group and click **Preview**.
8. Select **Apply machine filters to preview** and click **OK**.
9. Review the data in the **Non-compliant results** window to verify that your rule is behaving as expected. If the results are incorrect, adjust your rules and filters until they work correctly when you preview them.

What to do next

- If you have more than one rule that you must run in a particular order, set the order. The Set Order option is located on the toolbar.
- Create a template. See "Create Machine Group Compliance Templates" on page 187.

Create Machine Group Compliance Templates

You can create compliance templates that include one or more rule groups that assess your selected virtual or physical machine group to determine which machines are compliant and noncompliant.

This procedure demonstrates how to check whether your Linux machines, except those running 64-bit operating systems, have at least a 5GB hard drive capacity.

Prerequisites

Create a rule group. See "Create and Test Static Machine Group Compliance Rules" on page 184.

Procedure

1. Click **Compliance**.
2. Select **Machine Group Compliance > Templates**.
3. Click **Add**.
4. Type the name and description in the text boxes and click **Next**.

   For example, Disk Cap > 5 GB not 64bit.
5. Move the rule group to the list on the right and click **Next**.

   For example, Capacity 5GB - Linux and UNIX.
6. Select **Return both compliant and non-compliant** and click **Next**.

   Returning complaint and noncompliant results helps you determine whether your template is returning the correct results.
7. Review your changes and click **Finish**.

What to do next

Run the template. See "Run Machine Group Compliance Templates" on page 188.

Run Machine Group Compliance Templates

You run templates against your collected data to determine which virtual or physical machines are compliant or noncompliant.

When a compliance template is run, the results appear in a report format and a data grid format.

This procedure demonstrates how to check whether your Linux machines, except those running 64-bit operating systems, have at least a 5GB hard drive capacity.

Prerequisites

Create a template. See "Create Machine Group Compliance Templates" on page 187.

Procedure

1. Click **Compliance**.
2. Select **Machine Group Compliance > Templates**.
3. Select your template in the data grid and click **Run**.

   In this example, select Disk Cap > 5 GB not 64bit.
4. Click **OK**.
5. When the template run is finished, click **Close**.
6. Double-click the template name in the data grid.

   Unless you turned off the summary view, the Compliance Results report appears. The report includes the number of machines that are compliant and the number that are noncompliant.
7. To view the results in the data grid, click **View data grid**.

What to do next

- Evaluate the results and resolve any issues on the noncompliant objects. "Resolve Noncompliant Compliance Template Results" on page 189.
- If you find results that you want to temporarily make compliant or noncompliant, create an exception. See "Create Machine Group Compliance Exceptions" on page 191.

Resolve Noncompliant Compliance Template Results

The results for the compliance templates indicate whether the rules was compliant or noncompliant. To resolve noncompliant results, you might be able to enforce noncompliant results manually, by using VCM, or you can add an exception for expected noncompliant results.

These procedures provide a variety of examples that apply to machine group compliance, Active Directory compliance, and virtual environments compliance.

Procedure

1. "Enforce Compliance Template Results Using Enforceable Compliance" on page 189

   You can use enforceable compliance to resolve noncompliant results. Enforceable compliance is a VCM action that changes settings on physical machines, virtual machines, or virtual objects during or after a compliance template is run on the machine or object.

2. "Enforce Compliance Template Results by Using VCM Actions" on page 190

   You can resolve noncompliant results using VCM actions on the data grids to change settings when the action is not available for enforceable compliance.

3. "Manually Enforce Compliance Template Results" on page 191

   You can resolve noncompliant results by directly accessing the virtual or physical machine, or by accessing the object in vCenter Server, to change the noncompliant configuration setting.

4. "Create Machine Group Compliance Exceptions" on page 191

   Compliance exceptions are the method you use to temporarily or permanently override specific template results rather than resolve noncompliant results,

Enforce Compliance Template Results Using Enforceable Compliance

You can use enforceable compliance to resolve noncompliant results. Enforceable compliance is a VCM action that changes settings on physical machines, virtual machines, or virtual objects during or after a compliance template is run on the machine or object.

The enforceable compliance action is available for some, but not all, settings. You configure the action in the rule to allow automatic enforcement during the compliance run or to initiate enforcement after compliance.

If the rule is configured for automatic enforcement, VCM changes the noncompliant setting to the compliant value on the affected machine or object after the compliance assessment runs. If the rule is not configured for automatic enforcement, you select a noncompliant rule and enforce it. VCM then changes the value on the affected machine or object to the required compliant value.

For this example, you are working with a Windows or Linux machine, either a physical machine or a virtual machine.

This example assumes that you are not auto-enforcing the noncompliant results during the compliance run.

Procedure

1. Click **Compliance**.
2. Select **Machine Groups Compliance > Templates > {template name}**.
3. In the Status column, select the rule results that are noncompliant and enforceable, indicated by the NoncompliantEnforceable icon, and click **Enforce**.
4. Select **Selected items(s) only** and click **Next**.
5. Review the Information page to ensure that you understand the number of items affected by the enforcement change and click **Finish**.
6. After the enforcement job finishes, click **Refresh**.
7. In the Enforcement column, verify that the enforcement action succeeded, indicated by the Succeeded icon.

What to do next

Collect the appropriate data from the physical or virtual machines or objects and run compliance against the collected data. The machines or objects should now be compliant.

Enforce Compliance Template Results by Using VCM Actions

You can resolve noncompliant results using VCM actions on the data grids to change settings when the action is not available for enforceable compliance.

For this example, a template includes a rule that requires virtual machines to be powered on. If a virtual machine is powered off, the object is noncompliant. The compliance remediation action is to power it on.

Procedure

1. Click **Compliance**.
2. Select **Virtual Environments Compliance > Templates > {template name}**.
3. In the Status column, identify the rule results that are noncompliant.
4. Identify the affected physical or virtual machines or virtual objects, and determine the expected value of the property.

   For example, click and drag the Status column heading and the Rule column heading to the filter. Expand the noncompliant results and the rule related to the power state. The noncompliant object appears in the object column.
5. To resolve the noncompliant results, click **Console** and select **Virtual Environments**, the **Windows tab**, or the **UNIX tab**, and browse to the data grid where the action is available.

   For example, click **Console** and select **Virtual Environments > vCenter > Guests > Summary**.
6. Select the machines or objects that you identified as noncompliant and click the applicable action button on the data grid.

   For example, select the virtual machines that are powered off that should be powered on to be compliant and click **Power VM On**.
7. Follow the prompts to configure the options, select **Run action now**, and click **Finish**.

What to do next

Collect the appropriate data from the physical or virtual machines or objects and run compliance against the collected data. The objects should now be compliant.

Manually Enforce Compliance Template Results

You can resolve noncompliant results by directly accessing the virtual or physical machine, or by accessing the object in vCenter Server, to change the noncompliant configuration setting.

Procedure

- Using your allowed methods, change the noncompliant setting value on the machine or object to the required compliant value.

What to do next

Collect the appropriate data from the virtual or physical machines or objects and run compliance against the collected data. The objects should now be compliant.

Create Machine Group Compliance Exceptions

To temporarily or permanently override the specific template results, use exceptions rather than explicitly resolve noncompliant results.

The exceptions are defined against the template results and indicate that a specific result is compliant or noncompliant even though it does not match the requirements of the rules.

You can add exceptions only to existing templates.

This procedure demonstrates how to check whether your Linux machines, except those running 64-bit operating systems, have at least a 5GB hard drive capacity.

Prerequisites

Create a template. See "Create Machine Group Compliance Templates" on page 187.

Procedure

1. Click **Compliance**.
2. Select **Machine Group Compliance > Templates > template name**.
3. In the data grid, select the noncompliant result on which you are basing the exception and click **Add Exception**.

   For example, the noncompliant result is the RHEL_60_TestDev machine.
4. Type the name, short description, description, and sponsor in the text boxes and click **Next**.
5. Select the template to which you are applying the exception in the drop-down menu and click **Next**.

   For example, select Disk Cap > 5 GB not 64bit.
6. Select the machine group to which you are applying the exception and click **Next**.

   For this example, select All UNIX Machines.
7. Select the override options and the expiration date.
   a. Select **Override non-compliant results to compliant**.
   b. Select **No Expiration**.
   c. Click **Next**.
8. To define the exception values, modify, delete, or add to the properties, operators, and values for the

selected results.

In this example, to specify RHEL_60_TestDev as the exception, remove all the property rows, except for the row containing the Machine property.

9. Click **Finish**.

What to do next

- Run the template. See "Run Machine Group Compliance Templates" on page 188.
- Create alerts and schedule regular runs of your compliance templates. See "Configure Alerts and Schedule Machine Group Compliance Runs" on page 192.

Configure Alerts and Schedule Machine Group Compliance Runs

To optimize how VCM monitors the compliance of physical and virtual machines in your environment, configure alerts and schedule regular compliance template runs on your collected machine group data.

Prerequisites

Create at least one virtual environments compliance template. See "Create and Run Machine Group Compliance Templates" on page 182.

Procedure

1. "Create Machine Group Compliance Alert Rules" on page 192

   Alert rules are the conditions you define that determine when an alert is generated. Machine group alert rules are based on machine group compliance templates.

2. "Create Machine Group Compliance Alert Configurations" on page 193

   Machine group compliance alert configurations are created for machine groups to generate alerts when a machine group compliance template returns noncompliant results during scheduled runs of the template.

3. "Schedule Machine Group Compliance Template Runs" on page 193

   You can schedule a regular run of your machine group compliance templates to ensure that the collected data is regularly assessed for adherence to the defined compliance rules.

Create Machine Group Compliance Alert Rules

Alert rules are the conditions you define that determine when an alert is generated. Machine group alert rules are based on machine group compliance templates.

Prerequisites

Verify that you have machine group compliance templates. See "Create and Run Machine Group Compliance Templates" on page 182.

Procedure

1. Click **Administration**.
2. Select **Alerts > Rules**.
3. Click **Add**.
4. Type the alert name and description in the text boxes and click **Next**.
5. Select **Compliance Results Data** and click **Next**.

6. Select a compliance template and click **Next**.
7. Review the configured actions and click **Finish**.

What to do next

Create a virtual environments configuration that includes this rule. See "Create Machine Group Compliance Alert Configurations" on page 193.

Create Machine Group Compliance Alert Configurations

Machine group compliance alert configurations are created for machine groups to generate alerts when a machine group compliance template returns noncompliant results during scheduled runs of the template.

You must have at least one unused rule to add to the alert configuration parameters.

Prerequisites

- Verify that you have machine group alert rules. See "Create Machine Group Compliance Alert Rules" on page 192.
- Review the automated response options, which are available in the online Help.

Procedure

1. Click **Administration**.
2. Select **Alerts > Machine Group Configurations**.
3. In the middle pane, select the machine group for which you want to generate an alert if one or more rules in the template fail.
4. Click **Add**.
5. Select a machine group compliance results alert rule and click **Next**.
6. Select the alert severity and click **Next**.
7. Select and configure one or more automated responses that are performed when an alert is generated, and click **Next**.

   Depending on the automated responses you selected, the pages vary. See the online Help for configuration details.
8. Review the alert configuration, and click **Finish**.

What to do next

Schedule a job to run your the machine group compliance templates. See "Schedule Machine Group Compliance Template Runs" on page 193.

Schedule Machine Group Compliance Template Runs

You can schedule a regular run of your machine group compliance templates to ensure that the collected data is regularly assessed for adherence to the defined compliance rules.

Compliance templates are run against collected data, so you should also schedule collections for the data types and machine groups that you are assessing.

Prerequisites

- Schedule a regular collection of the data types for the machine groups against which you are running the machine group compliance templates. For example, see "Configure Scheduled Linux, UNIX, and Mac OS X Collections" on page 133.
- Create machine group compliance templates. See "Create and Run Machine Group Compliance Templates" on page 182.
- Create machine group compliance alerts. See "Create Machine Group Compliance Alert Rules" on page 192.

Procedure

1. Click **Administration**.
2. Select **Job Manager > Scheduled**.
3. Click **Add**.
4. Select **Compliance** and click **Next**.
5. Type a name and description in the text boxes and click **Next**.
6. Select the machine group template and click **Next**.
7. Select the machine groups against which to run the template assessment and click **Next**.
8. Configure frequency, time of day, and duration for the job and click **Finish**.
9. To test whether the job is producing the expected results, click **Run Now** on the data grid toolbar. Otherwise, the job runs at the scheduled time.

What to do next

If you configured a machine compliance alert for this template, and noncompliant rules were found, you can review any alerts in the Alerts node in the Console.

Getting Started with SCAP Compliance

Security Content Automation Protocol (SCAP) is a suite of standards that enable automated vulnerability management, measurement, and policy compliance evaluation. The VCM SCAP implementation employs or references six open standards that SCAP uses to enumerate, evaluate, and measure the impact of software problems and to report results.

- **Common Configuration Enumeration (CCE)**. A standard of unique identifiers for common system configuration issues
- **Common Vulnerabilities and Exposures (CVE)**. A dictionary of standard identifiers for security vulnerabilities related to software flaws
- **Open Vulnerability and Assessment Language (OVAL)**. An XML standard for security testing procedures and reporting
- **Common Platform Enumeration (CPE)**. Standard identifiers and a dictionary for platform and product naming
- **Extensible Configuration Checklist Description Format (XCCDF)**. A standard for specifying checklists and reporting results
- **Common Vulnerability Scoring System (CVSS)**. A standard for conveying and scoring the impact of

vulnerabilities

To calculate CVSS scores that apply to your unique environment, go to the CVSS scoring Web site, fill in the form, and click the Update Scores button.
http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2

This release of VCM is compatible with the SCAP 1.0 validation program and is for Windows platforms only.

Conduct SCAP Compliance Assessments

You import a benchmark, run an SCAP assessment on the managed machines in your environment, review the results, and have the option to export the results.

Procedure

1. "Import an SCAP Benchmark" on page 195

   Add the SCAP benchmark to VCM so that you have the industry-approved set of compliance checks against which to assess your managed machines.

2. "Run an SCAP Assessment" on page 196

   Run an SCAP assessment that compares your managed machine configuration against a profile in a standard SCAP benchmark.

3. "View SCAP Assessment Results" on page 196

   Open and search SCAP assessment results through access in the data grid for the profile against which you measured managed machines.

4. "Export an SCAP Assessment" on page 196

   You can export assessment result output to HTML, XML, CSV, and log files.

Import an SCAP Benchmark

Add the SCAP benchmark to VCM so that you have the industry-approved set of compliance checks against which to assess your managed machines.

Prerequisites

Obtain a copy of the Tier III or Tier IV benchmark bundle ZIP file that you want. The National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) provides benchmarks for download.
http://web.nvd.nist.gov/view/ncp/repository

Procedure

1. Copy the bundle ZIP file to the following folder.

   ```
   \\machine-name\CMFiles$\SCAP\Import
   ```

2. Click **Compliance**.
3. Select **SCAP Compliance > Benchmarks**.
4. Click **Import**.
5. Highlight the bundle, and click the right arrow to select it for import.
6. Click **Next**.
7. Review your selections and click **Finish**.

Run an SCAP Assessment

Run an SCAP assessment that compares your managed machine configuration against a profile in a standard SCAP benchmark.

Prerequisites

Import the benchmark. See "Import an SCAP Benchmark" on page 195.

Procedure

1. Click **Compliance**.
2. Select **SCAP Compliance > Benchmarks >** ***benchmark name*** **>** ***profile name***.
3. Click **Run Assessment**.
4. Highlight the machines to assess, and click the down arrow to select them.
5. Click **Next** and click **Next** again.
6. Click **Next**, review your selections, and click **Finish**.

   A collection job starts, and results are not available until the job finishes. The process differs from the general VCM compliance feature, which looks at existing collection data in the database.

View SCAP Assessment Results

Open and search SCAP assessment results through access in the data grid for the profile against which you measured managed machines.

Where appropriate, VCM includes the corresponding standard identifier in its SCAP assessment results and provides an embedded hyperlink to information about the identifier on Web pages such as those provided by MITRE.

Prerequisites

Generate an assessment. See "Run an SCAP Assessment" on page 196.

Procedure

1. Click **Compliance**.
2. Select **SCAP Compliance > Benchmarks >** ***benchmark name*** **>** ***profile name***.
3. In the data grid, find the row for the machine for which you generated an assessment.
4. In the row, click the ellipsis button for the result format that you generated.

   The following format options are available on the data grid.

   OVAL HTML
   OVAL XML
   XCDDF HTML
   XCDDF XML

5. In the browser window that displays the assessment result, press **Ctrl+f** to open the search feature, and find the results in which you are interested.

Export an SCAP Assessment

You can export assessment result output to HTML, XML, CSV, and log files. CSV is used for CCE pass/fail results, and log files are for troubleshooting.

Upon successful export, VCM creates a file with a name based on the machine name, output format, and time stamp in the following folder on the Collector.

`\\{`*machine-name*`}\CMFiles$\SCAP\Export`

You can export the formats that are viewable from the data grid, as well as others.

Prerequisites

Run the assessment. See "Run an SCAP Assessment" on page 196.

Procedure

1. Click **Compliance**.
2. Select **SCAP Compliance > Benchmarks >** ***benchmark name*** **>** ***profile name***.
3. Click **Export**.
4. Highlight the machine for which you want to export assessment results, and click the down arrow to select it.
5. Click **Next**.
6. Select the output and format for the export file, and click **Finish**.

Provisioning Physical or Virtual Machine Operating Systems 11

Operating system (OS) provisioning is the process of installing operating systems to physical or virtual machines. As part of the provisioning process, you can add newly provisioned machines to VCM.

OS provisioning enables you to quickly deploy one or more physical or virtual machines to meet expanding business needs. Some of these machines may have limited use and lifespan, and may be reprovisioned for other purposes. Other machines are provisioned and distributed for long term use.

The provisioning process installs the supported operating system and the VCM Agent. When the target machines are licensed, you can collect machine data, monitor the machines' state and status, and manage the security and compliance of the machines.

This chapter includes the following topics:

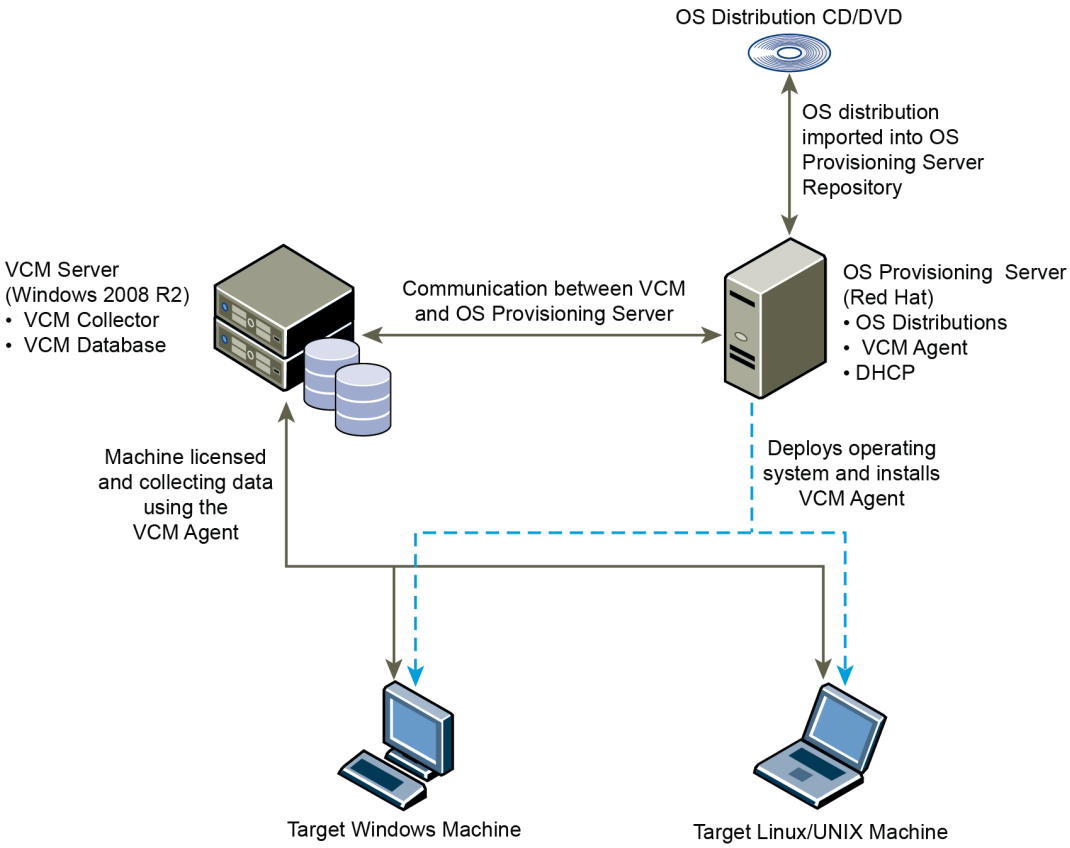
Operating System Provisioning Components 199
Configure Operating System Provisioning Servers 201
Provision Machines with Operating System Distributions 204
Provisioned Machines Results 213
Reprovision Machines 214

Operating System Provisioning Components

The OS provisioning components include the VCM Collector, one or more OS Provisioning Servers, and the target physical or virtual machines.

The OS Provisioning Server, when it is installed and configured in your environment, serves as the engine for OS provisioning. However, the process of initiating provisioning actions is managed through the VCM Console. See Figure 11–1. Relationship of OS Provisioning Components.

Figure 11–1. Relationship of OS Provisioning Components


OS Distribution CD/DVD
OS distribution imported into OS Provisioning Server Repository
VCM Server (Windows 2008 R2)
• VCM Collector
• VCM Database
Communication between VCM and OS Provisioning Server
OS Provisioning Server (Red Hat)
• OS Distributions
• VCM Agent
• DHCP
Machine licensed and collecting data using the VCM Agent
Deploys operating system and installs VCM Agent
Target Windows Machine
Target Linux/UNIX Machine

Patching the Operating System Provisioning Server

Exclude the OS Provisioning Server instances from your automated patching in VCM. Patching the operating system will elevate the minor version and may leave the OS Provisioning Server in an unsupported state.

How Operating System Provisioning Works

The process of provisioning operating systems on physical or virtual machines includes actions that you run in VCM, actions that you perform outside VCM, the underlying processes associated with the actions, and the results.

1. Use VCM to collect the available OS distributions from the OS Provisioning Server.

   The collected distributions are displayed in the OS Distributions data grid and are available to install on target machines.

2. Set the BIOS on the target machines to network boot.
3. Connect the target machines to the provisioning network and turn them on.

   The OS Provisioning Server discovers the available target machines.

4. Use VCM to collect the discovered target machines from the OS Provisioning Server.

   The discovered target machines appear in the Provisionable Machines data grid by MAC address.

5. Use VCM to send the command that includes the provisioning details to the OS Provisioning Server to

provision the target machines.

The OS Provisioning Server creates an installation session for the target machines based on the configured OS distribution settings.

6. Reboot the target machines.

   As each target machine requests an IP address from the DHCP server and requests a PXE boot, OS Provisioning Server checks the machine's MAC address to determine if the machine has an installation session waiting on the OS Provisioning Server. If an installation session for the machine is found, the OS installer boots over TFTP, the OS distribution and VCM Agent are downloaded to the target machines using HTTP, and the distribution and Agent are installed on the target machines.

   When the installation completes, the new physical or virtual machines appear in the Provisioned Machines data grid. They are licensed or available to license in VCM. If the machine is not licensed, you must license it to manage the machine. As each machine is licensed, you manage it in VCM as a Windows or Linux machine.

Configure Operating System Provisioning Servers

Add OS Provisioning Server instances to VCM so that you can use VCM to submit the install operating system actions to the OS Provisioning Server. It is the OS Provisioning Server instances that install the imported operating systems on the target physical or virtual machines.

Prerequisites

- Install the OS Provisioning Server and import the OS distributions. See the VCM Advanced Installation Guide.
- Install the VCMAgent CMAgent.5.5.0.Linux on your OS Provisioning Server machines using HTTP communication protocol and port 26542, the default port. See "Install the VCM Agent on Linux, UNIX, and Mac OS X Operating Systems" on page 125.
- Collect the Machines - General data type from the OS Provisioning Server machine. See "Collect Linux, UNIX, and Mac OS X Data" on page 132.

Procedure

1. "Add Operating System Provisioning Servers" on page 202

   To register the OS Provisioning Servers, you must add the Red Hat servers that you configured as OS Provisioning Servers. When the servers are registered, you select the OS Provisioning Server from which to install operating systems when you are configuring the provisioning action.

2. "Set the Trust Status for Operating System Provisioning Servers" on page 202

   You set the trusted status is on Agent machines where you verify that the connection is legitimate. When you set the trust status, you are marking the Agent certificate as trusted. When transmitting sensitive information, such as credentials, between the Collector and OS Provisioning Servers, the machines must be trusted.

3. "Collect Operating System Distributions" on page 203

   Collect the OS Distributions to ensure that you have access to all the operating systems in the OS Provisioning Server repository.

4. "Discover Provisionable Machines" on page 203

   The OS Provisioning Server identifies provisionable physical or virtual machines in your environment

when the target machines are set to network boot and attempt to PXE boot.

5. "Provision Machines with Operating System Distributions" on page 204

   The OS provisioning process installs one Windows or Linux operating system distribution on one or more physical or virtual machines using OS provisioning.

Continuous provisioned machine management is based on the latest data you collect from the OS Provisioning Server. See "Provisioned Machines Results" on page 213.

Add Operating System Provisioning Servers

To register the OS Provisioning Servers, you must add the Red Hat servers that you configured as OS Provisioning Servers. When the servers are registered, you select the OS Provisioning Server from which to install operating systems when you are configuring the provisioning action.

Prerequisites

- Verify that you installed and configured your OS Provisioning Server instances. See the *VCM Advanced Installation Guide*.
- Ensure that the Red Hat servers that you configured as OS Provisioning Server are added and licensed in VCM. See "Configure Collections from Linux, UNIX, and Mac OS X Machines" on page 120.
- Ensure that you collected Machines - General data from your OS Provisioning Server instances. See "Collect Linux, UNIX, and Mac OS X Data" on page 132.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > OS Provisioning > Registered Servers**.
3. Click **Add**.
4. On the Select OSP Server page, move the selected servers to the lower pane and click **Next**.
5. Review the Confirmation information and click **Finish**.
6. Click **Refresh**, located on the main toolbar, to update the data grid.

What to do next

Collect the available distributions from the target OS Provisioning Servers. See "Collect Operating System Distributions" on page 203.

Set the Trust Status for Operating System Provisioning Servers

You set the trusted status is on Agent machines where you verify that the connection is legitimate. When you set the trust status, you are marking the Agent certificate as trusted. When transmitting sensitive information, such as credentials, between the Collector and OS Provisioning Servers, the machines must be trusted.

If you choose not to use this level of security, you can set the **Allow sensitive parameters to be passed to agents not verified as Trusted** option to `Yes` in the General Settings for the Collector data grid.

Prerequisites

Verify that your OS Provisioning Server instances are added as registered servers. See "Add Operating System Provisioning Servers" on page 202.

Procedure

1. Click **Administration**.
2. Select **Certificates**.
3. Select the OS Provisioning Server machines and click **Change Trust Status**.
4. Add any additional OS Provisioning Server instances to trust to the lower data grid.
5. Select **Check to trust or uncheck to untrust the selected machines** and click **Next**.
6. Review the number of machines affected and click **Finish**.

What to do next

Collect OS distributions from your OS Provisioning Server instances. See "Collect Operating System Distributions" on page 203.

Collect Operating System Distributions

Collect the OS Distributions to ensure that you have access to all the operating systems in the OS Provisioning Server repository. These OS Distributions are operating system images that are available to install on target machines.

Prerequisites

- Ensure that operating system distributions are imported into the OS Provisioning Server repository. To import OS distributions, see See the *VCM Advanced Installation Guide*.
- Verify that the OS Provisioning Integration Enabled setting is configured with a value greater than 0. Click **Administration** and select **Settings > OS Provisioning Settings > OS Provisioning Server**.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > OS Provisioning > OS Distributions**.
3. Click **Refresh**.

   This action collects data from the OS Provisioning Server. When the collection finishes, the available operating systems distributions appear in the data grid.

What to do next

Discover target machines. See "Discover Provisionable Machines" on page 203.

Discover Provisionable Machines

The OS Provisioning Server identifies provisionable physical or virtual machines in your environment when the target machines are set to network boot and attempt to PXE boot.

Prerequisites

- Ensure that the target machines have a minimum of 1GB RAM and meet the minimum RAM requirements for the operating system you are installing.
- Configure the primary network interface on the target machines with a connection to the OS Provisioning Server deployment network. If you use a different network as the primary interface, the deployment process appears to start, but you receive communication errors and the process ultimately fails.

Procedure

1. On target machines, configure the BIOS to network boot.
2. Start the machines on your provisioning network.
3. In VCM, click **Administration**.
4. Select **Machines Manager > OS Provisioning > Provisionable Machines**.
5. On the data grid toolbar, click **Refresh**.

   This action collects data from the OS Provisioning Server and the provisionable machines appear in the data grid when the collection is finished. The machines are identified by MAC address.

What to do next

Provision the target machine. See "Provision Machines with Operating System Distributions" on page 204.

Provision Machines with Operating System Distributions

The OS provisioning process installs one Windows or Linux operating system distribution on one or more physical or virtual machines using OS provisioning.

Depending on the distribution you are installing, use one of the following procedures.

- "Provision Windows Machines" on page 204

  Provisioning physical or virtual machines with a Windows operating system installs the selected operating system and the VCM Agent on one or more of your Windows machines.

- "Provision Linux Machines" on page 208

  Provisioning physical or virtual machines with a Linux operating system installs the selected operating system and the VCM Agent on one or more of your Linux machines.

Provision Windows Machines

Provisioning physical or virtual machines with a Windows operating system installs the selected operating system and the VCM Agent on one or more of your Windows machines.

You can install one OS distribution on one or more target machines. To install a different OS distribution, configure a new OS provisioning action.

Select no more than ten machines per provisioning action.

Prerequisites

- Verify that the operating system you are installing is compatible with the hardware or configuration of the target physical or virtual machines. For example, the operating system must support the drivers required by the hardware.
- Verify that the OS Provisioning Servers are registered. See "Add Operating System Provisioning Servers" on page 202.
- Verify that the OS distributions are collected and appear in the OS Distributions data grid. See "Collect Operating System Distributions" on page 203.
- Verify that the target machines are discovered and appear in the Provisionable Machines data grid. See "Discover Provisionable Machines" on page 203.

- Identify or create any postinstallation scripts that you want to run on the target machine after it is provisioned with the new operating system. The postinstallation scripts are copied to the target machine along with the OS distribution and runs after the operating system is installed.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > OS Provisioning > Provisionable Machines**.
3. Select one or more target machines in the data grid on which you are installing the same OS distribution.
4. Click **Provision**.
5. On the Select OSP Server page, select the OS Provisioning Server that will manage the provisioning action and click **Next**.
6. On the Select Machines page, add or remove target machines from the selected machine list and click **Next**.

7. On the Select OS Distribution page, select the Windows operating system that you are installing on the selected machines and click **Next**.
8. On the Settings page, configure the options required for your selected Windows OS distribution and click **Next**.

Option	Description
Product License Key	(Optional for Windows 2008. Required for Windows 2003 and Windows 7.) Type a license matching the operating system you are installing.
License Key Type	(Required for Windows 2003 and Windows 7, and for Windows 2008 if Product License Key is provided.) Select the license type, either Retail or MAK (multiple activation key).
Admin Password	(Required) Type the password for the target machines' local Administrator account.
Re-enter Admin Password	(Required) Retype the password.
Domain or Workgroup	(Required) If a Domain and Domain User are specified, Domain details are used. If the domain details are not provided, then the Workgroup is used.
Add machine(s) to a Domain	Select the check box to add the machines to a Domain rather than a Workgroup. If you select this option, you must configure the domain details. The domain controller must be accessible to the deployed machine during the provisioning process.
Domain Type	Available if you select Add machine(s) to a Domain. Select the type in the drop-down menu.
Domain User	Available if you select Add machine(s) to a Domain. Type a user name.
Domain User Password	Available if you select Add machine(s) to a Domain. Type a password for the specified Domain User.
Re-enter Domain User Password	Available if you select Add machine(s) to a Domain. Retype the password.
Organization	Name of the licensing organization.
Windows SKU	(Window 2008 and Windows 7 only) Select the value in the drop-down list. See the online help for possible values.

Option	Description
Use DHCP to determine IP address	Use your designated DHCP to assign IP address, subnet, default gateway, and DNS. If not selected, you must manually add the information on the Machine-Specific Settings page.
License these machines for VCM	License the machines for VCM management.

9. On the Machine-Specific Settings page, type the **HostName** and click **Next**.

   The HostName is limited to 15 characters.

   If you did not select **Use DHCP to determine IP address** on the Settings page, you must configure the IP Address, Subnet, Default Gateway, and DNS.

10. (Optional) On the Post-install Script page, type a **Script Name** and the script, and click **Next**.

11. (Optional) On the Disk Configuration page, select one of the options and click **Next**.

Option	Description
Use all available disk space	Creates and formats a single partition using all the available disk space.
Create partition with *nn* GB.	Partitions and formats the specified space. The space you specify must be less than the total available space.

12. On the Confirmation page, click **Finish**.

    The OS Provisioning Server starts jobs for each of the selected target machines. Each job creates a configured session for the specified machines. The configured session includes information about the target machine, the OS distribution, the configuration information for the selected combination of target machine and operating system, and the VCM Agent.

13. Reboot the target machines.

    You must cycle the power on the machines either manually or using a remote administration mechanism. The machines must be configured to network boot from the OS Provisioning Server, which identifies the configured session that is waiting and the installation begins. If the session does not exist, then the target machine remains provisionable and is not provisioned until a session is created and the target machine is rebooted.

What to do next

- Verify that the provisioning process has begun. Click Administration and select **Machines Manager > OS Provisioning > Provisionable Machines**. The machines appear in the appropriate Available Machines or Licensed Machines data grid with an OS provisioning status of OS Provisioning Queued.
- Verify that the provisioning process is finished. Click **Administration** and select **Machines Manager > OS Provisioning > Provisioned Machines**. The OS provisioning status is OS Provisioning Succeeded or OS Provisioning Overwritten.
- Configure the Windows 2008 SP2, and R2, and Windows 7 machines on a public network with access to the Internet and manually complete the Windows license activation on the provisioned machines.
- (Optional) Change the Agent communication protocol. See "Change Agent Communication" on page 213.

Provision Linux Machines

Provisioning physical or virtual machines with a Linux operating system installs the selected operating system and the VCM Agent on one or more of your Linux machines.

You can install one OS distribution on one or more target machines. To install a different OS distribution, configure a new OS provisioning action.

Prerequisites

- Verify that the operating system you are installing is compatible with the hardware or configuration of the target physical or virtual machines. For example, the operating system must support the drivers required by the hardware.
- Verify that the OS Provisioning Servers are registered. See "Add Operating System Provisioning Servers" on page 202.
- Verify that the OS distributions are collected and appear in the OS Distributions data grid. See "Collect Operating System Distributions" on page 203.
- Verify that the target machines are discovered and appear in the Provisionable Machines data grid. See "Discover Provisionable Machines" on page 203.
- Identify or create any postinstallation scripts that you want to run on the target machine after it is provisioned with the new operating system. The postinstallation scripts are copied to the target machine along with the OS distribution and runs after the operating system is installed.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > OS Provisioning > Provisionable Machines**.
3. Select one or more target machines in the data grid on which you are installing the same OS distribution.
4. Click **Provision**.
5. On the Select OSP Server page, select the OS Provisioning Server that will manage the provisioning action and click **Next**.
6. On the Select Machines page, add or remove target machines from the selected machine list and click **Next**.

7. On the Select OS Distribution page, select the a Linux operating system that you are installing on the selected machines and click **Next**.
8. On the Settings page, configure the options required for your selected Linux OS distribution and click **Next**.

Option	Description
Product License Key	Type the license to use when installing the operating system on the target machines. The license must match the operating system you are installing.
Root Password	(Required) Type the password you are assigning to the local root.
Re-enter Root Password	(Required) Retype the password.
Domain	(Required) Type the domain to which you are assigning the machines.
Use DHCP to determine IP address	Use your designated DHCP to assign IP address, subnet, default gateway, and DNS. If this option is not selected, you must manually enter the information on the Machine-Specific Settings page.
License these machines for VCM after deployment	License the target machines for VCM management.

9. On the Machine-Specific Settings page, type the **HostName** and click **Next**.

   The HostName is limited to 32 characters.

   If you did not select **Use DHCP to determine IP address** on the Settings page, you must configure the IP Address, Subnet, Default Gateway, and DNS.
10. (Optional) On the Post-Install Script page, type a **Script Name**, the script, and click **Next**.

    Post-install scripts are copied to the machine when the OS distribution is copied and runs after the operating system is installed.
11. (Optional) On the Disk Configuration page, configure the options and click **Next**.

    You can either install the operating system without partitioning the disk, or you can create partitions and specify the size.

Option	Description
Custom Volume Plan	Select the check box to partition the disk.

Option	Description
Mount Point	Type the location of the mount point for the partition. For example, /, /boot, /usr, /var/log. You use the first partition for the operating system and then specify a second mount point for user home directories. The mount points value must meet the specific criteria. ■ / and /boot are required mount points. ■ Duplicate mount points are not allowed. ■ For a swap partition, the mount point and the file system type should be swap. ■ When naming mount points, you can use letters, digits, ., -, _, and +. Spaces are not allowed.
Volume Name	Type the name of the logical partition. For example, LogVol00. The volume names must meet specific criteria. ■ When naming volumes, you can use letters, digits, ., or _. Spaces are not allowed. ■ The name limit 16 characters. ■ If you assign a volume name, you must assign a volume group name. ■ If you assign more than one volume name in a volume group, you cannot use the same name for each volume name.
Volume Size	The the size of the partition in megabytes or gigabytes. For example, 10MB or 1GB. If you select **Grow partition to use all remaining space**, you can specify a value of 0MB. If Grow is not selected, you must specify a valid partition size.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>File System</td><td>Select the type of file system.
For a swap partition, the mount point and the file system type should be swap.
Supported File System options by operating system.

<table>
<tr><th>Operating System</th><th>Supported File System</th><th>swap</th><th>/boot</th><th>/</th><th>/home, /tmp, /usr, /var, /usr/local</th></tr>
<tr><td>RHEL 6.0</td><td>ext2, ext3, ext4, swap, vfat, xfs</td><td>swap</td><td>ext2, ext3, ext4</td><td>ext2, ext3, ext4</td><td>ext2, ext3, ext4,xfs</td></tr>
<tr><td>RHEL 5.4 and 5.5</td><td>ext2, ext3, ext4, swap, vfat</td><td>swap</td><td>ext2, ext3</td><td>ext2, ext3, ext4</td><td>ext2, ext3, ext4</td></tr>
<tr><td>RHEL 5.0 and 5.2</td><td>ext2, ext3, swap, vfat</td><td>swap</td><td>ext2, ext3</td><td>ext2, ext3</td><td>ext2, ext3</td></tr>
<tr><td>SLES 10.0 and 11.1</td><td>reiser, ext2, ext3, xfs, jfs, swap</td><td>swap</td><td>reiser, ext2, ext3, xfs, jfs</td><td>reiser, ext2, ext3, xfs, jfs</td><td>reiser, ext2, ext3, xfs, jfs</td></tr>
</table>
</td></tr>
<tr><td>Volume Group Name</td><td>Type the name of the logical group.
For example, VolGroup00. You can specify only one volume group on the target machines. You may add volume groups after the OS distribution is installed.
The volume names must meet specific criteria.
■ When naming volumes, you can use letters, digits, ., or _. Spaces are not allowed.
■ The name limit 16 characters.
■ If you assign a volume name, you must assign a volume group name.
■ (SLES only) You can assign only one volume group when partitioning the disk.
■ (RHEL 5.x and 6.0, and SLES 10.3 and 11.1 only) You cannot use /boot as part of the volume group name.</td></tr>
<tr><td>Add</td><td>Click to add the configuration data to the Custom Volume Plan list.</td></tr>
<tr><td>Custom Volume Plan list</td><td>Displays the disk configuration data.</td></tr>
</table>

Option	Description
Grow partition to use all remaining space	Select the option to allow the logical volume to fill available space up to the maximum size specified for the volume. You can select the option for only one partition. If you select this option, you can specify a Volume Size of 0MB.
Remove	Click to delete the selected row from the custom volume plan list.

12. On the Confirmation page, click **Finish**.

    The OS Provisioning Server starts jobs for each of the selected target machines. Each job creates a configured session for the specified machines. The configured session includes information about the target machine, the OS distribution, the configuration information for the selected combination of target machine and operating system, and the VCM Agent.

13. Reboot the target machines.

    You must cycle the power on the machines either manually or using a remote administration mechanism. The machines must be configured to network boot from the OS Provisioning Server, which identifies the configured session that is waiting and the installation begins. If the session does not exist, then the target machine remains provisionable and is not provisioned until a session is created and the target machine is rebooted.

What to do next

- Verify that the provisioning process has begun. Click Administration and select **Machines Manager > OS Provisioning > Provisionable Machines**. The machines appear in the appropriate Available Machines or Licensed Machines data grid with an OS provisioning status of OS Provisioning Queued.
- Verify that the provisioning process is finished. Click **Administration** and select **Machines Manager > OS Provisioning > Provisioned Machines**. The OS provisioning status is OS Provisioning Succeeded or OS Provisioning Overwritten.
- Move the Linux machine to your production network and synchronize the network time. See "Synchronize Time on Installed Linux Operating Systems" on page 212.
- (Optional) Change the Agent communication protocol. See "Change Agent Communication" on page 213.

Synchronize Time on Installed Linux Operating Systems

When Linux machines are provisioned with an operating system, the Network Time Protocol (NTP) service is not running. After moving the newly provisioned Linux machines to a network with access to the NTP server, you must synchronize the time on the machines to network time.

Prerequisites

- Configure the Linux machines on a network with access to the NTP server.
- Identify the NTP servers used in your environment.

Procedure

1. On the Linux machine, log in as `root`.
2. Run the `ntpdate -u <ntpserver>` command to update the machine clock.

   For example, `ntpdate -u ntp-time.for.mydomain`.
3. Open the `/etc/ntp.conf` file and add the NTP servers used in your environment.

   You can add multiple NTP servers similar to these examples.

   ```
   server ntp-time.for.mydomain

   server otherntp.server.org

   server ntp.research.gov
   ```
4. Run the `service ntpd start` command to start the NTP service and implement you configuration changes.

Change Agent Communication

The VCM Agent is installed by the OS Provisioning Server with default settings. After the operating system distribution is installed, you can change the communication setting or install a new Agent.

Prerequisites

Install Windows or Linux operating system distribution. See "Provision Windows Machines" on page 204 or "Provision Linux Machines" on page 208.

Procedure

1. Configure the communication settings for the machines on which you installed one of the following operating using OS provisioning.
   - The Windows Agent is installed with DCOM as the communication protocol. To change the protocol, click **Administration** and then select **Machines Manager > Licensed Machines > Licensed Windows Machines > Change Protocol**.
   - The Linux Agents are installed with inetd or xinetd, as appropriate, with a default communication port of 26542. To change any Agent settings, uninstall the Agent from the machine, and reinstall it with the settings you require. See "Configure Collections from Linux, UNIX, and Mac OS X Machines" on page 120.

Provisioned Machines Results

Review the OS provisioning data that is specific to the provisioning process.

After you provision the target machines, VCM manages them as Windows or Linux machines. As managed machines, you collect data, add software, run patching assessments, and apply rules to maintain machine compliance in your environment.

The displayed data is only as current as the last time you collected from the OS Provisioning Server.

Option	Description
Administration	View administrative details about the OS Provisioning Server. ■ To view all provisioned machines, click **Administration** and select **Machines Manager > OS Provisioning > Provisioned Machines**. ■ To view the provisioned Windows machines, click **Administration** and select **Machines Manager > Licensed Machines > Licensed Windows Machines**. The OS Provisioning Status column indicates whether the Windows machine was create using OS provisioning. ■ To view the provisioned Linux machines, click **Administration** and select **Machines Manager > Licensed Machines > Licensed UNIX Machines**. The OS Provisioning Status column indicates whether the Linux machine was create using OS provisioning.

Reprovision Machines

You can reprovision Windows or Linux machines where the operating system was installed using the OS Provisioning Server and VCM.

When machines are reprovisioned, you may change the machine name.

CAUTION Reprovisioning overwrites the existing disk with a new operating system. All existing data is lost.

Prerequisites

- Verify that the machine to be reprovisioned is listed in the Provisioned Machines data grid. Select **Administration** and click **Machines Manager > OS Provisioning > Provisioned Machines**.
- Review the provisioning process for the OS distribution you are installing. See "Provision Machines with Operating System Distributions" on page 204.
- On the target machine, set the BIOS to network boot.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > OS Provisioning > Provisioned Machines**.
3. Select the machines.
4. Click **Re-provision**.
5. On the Select OSP Server page, select the OS Provisioning Server that will manage the provisioning action and click **Next**.
6. On the **Select Machines** page, add or remove machines and click **Next**.
7. On the **Select OS Distribution** page, select the operating system you are installing on the selected machines and click **Next**.
8. Continue with the provisioning wizard.

   The wizard options vary depending on the OS distribution you are installing.

9. When you are certain that the selected machines are those you want to reprovision, select the **Proceed with re-provisioning of the operating system on the selected machines** check box.
10. Click **Finish**.

    The OS Provisioning Server starts jobs for each of the selected machines. Each job creates a configured session for the specified machines. The configured session includes information about the target machine, the OS distribution, the user configuration information for the selected combination of machine and operating system, and the VCM Agent.
11. Reboot the target machines.

    You must the cycle the power on the machines either manually or using some remote administration mechanism. The machines must be configured to network boot from the provisioning network. If a session is waiting on the OS Provisioning Server, the installation begins. If the session does not exist, then the machine remains provisioned and will not be re-provisioned until the session is created.

What to do next

- Verify that the provisioning process has begun. Click Administration and select **Machines Manager > OS Provisioning > Provisionable Machines**. The machines appear in the appropriate Available Machines or Licensed Machines data grid with an OS provisioning status of OS Provisioning Queued.
- Verify that the provisioning process is finished. Click **Administration** and select **Machines Manager > OS Provisioning > Provisioned Machines**. The OS provisioning status is OS Provisioning Succeeded or OS Provisioning Overwritten.
- Configure the Windows 2008 SP2, and R2, and Windows 7 machines on a public network with access to the Internet and manually complete the Windows license activation on the provisioned machines.
- (Optional) Change the Agent communication protocol. See "Change Agent Communication" on page 213.

Provisioning Software on Managed Machines 12

Software provisioning is the process you use to create software packages, publish the packages to repositories, and then install packages on one or more target machines.

To support the provisioning process, the VCM Software Provisioning components consist of VMware vCenter Configuration Manager Package Studio, software package repositories, and Package Manager.

For more information about software provisioning, see VCM online Help, the *VCM Software Provisioning Components Installation and User's Guide*, and the Package Studio online Help.

This chapter includes the following topics:

- Install the Software Provisioning Components 218
- Using Package Studio to Create Software Packages and Publish to Repositories 223
- Using VCM Software Provisioning for Windows 225
- Related Software Provisioning Actions 229

Using Package Studio to Create Software Packages and Publish to Repositories

Package Studio is the application used to build software packages for installation on target Windows servers and workstations.

Windows packages can include in-house and commercial software installation files, including .msi, .exe, VBScripts, python, PowerShell.

To add a software installer to a package, it must be able to install and uninstall unmanned or quietly using command line options, response files, or other similar methods.

Software Repository for Windows

Software Repository for Windows is the shared location to which packages are published by Package Studio and the location from which Package Manager downloads packages for installation.

Package Manager for Windows

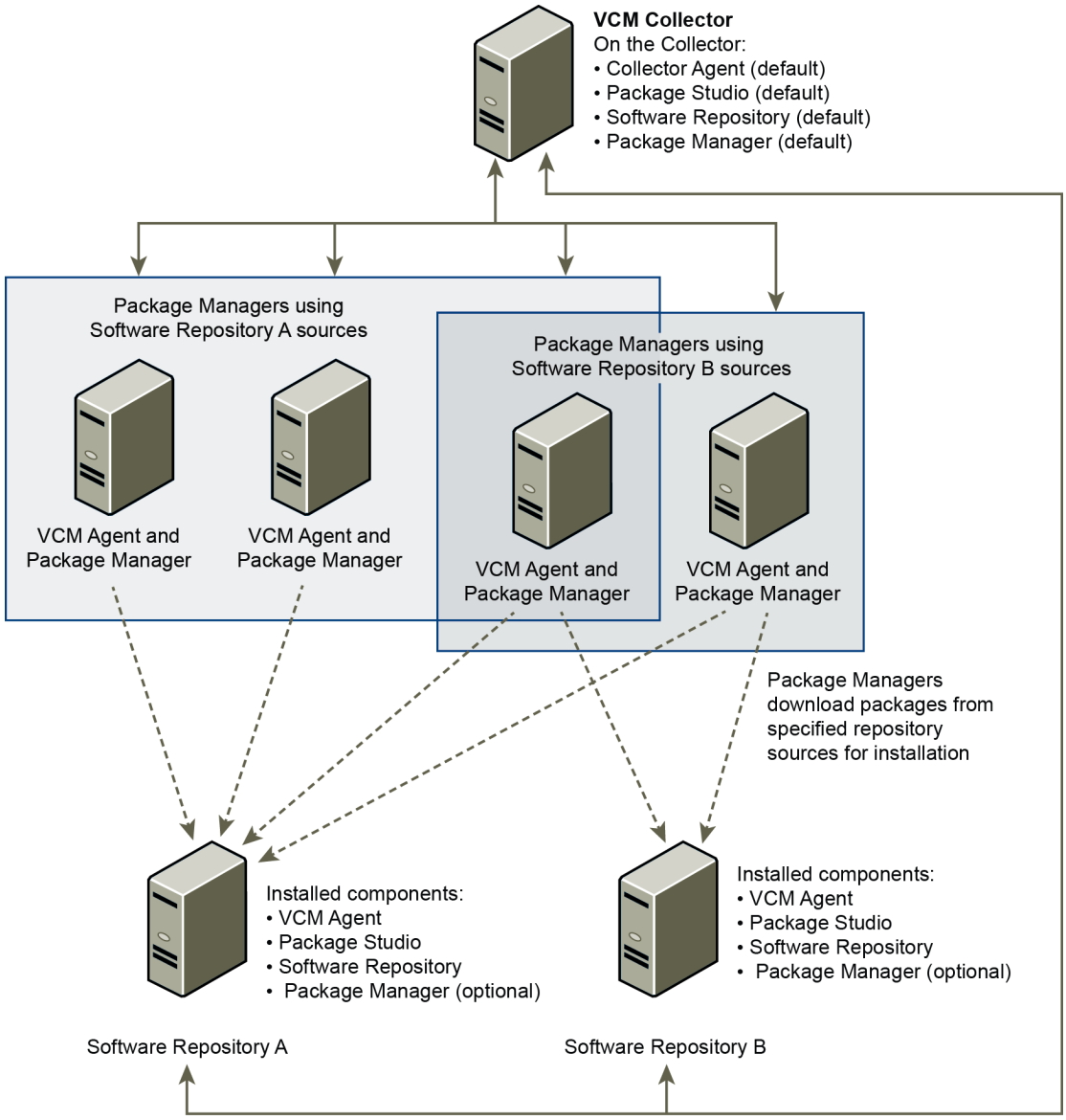
Package Manager is the application installed on each machine to manage the installation and removal of the software contained in packages. Package Manager is configured to use one or more repositories as sources for packages.

If you are using the software provisioning components in conjunction with VMware vCenter Configuration Manager (VCM), you can use VCM to add and remove sources, and to install and remove packages.

Software Provisioning Component Relationships

The following diagram displays the general relationship between Package Studio, repositories, and Package Manager in a working environment.

Figure 12–1. Software Provisioning Diagram


VCM Collector
On the Collector:
• Collector Agent (default)
• Package Studio (default)
• Software Repository (default)
• Package Manager (default)
Package Managers using Software Repository A sources
Package Managers using Software Repository B sources
VCM Agent and Package Manager
VCM Agent and Package Manager
VCM Agent and Package Manager
VCM Agent and Package Manager
Package Managers download packages from specified repository sources for installation
Installed components:
• VCM Agent
• Package Studio
• Software Repository
• Package Manager (optional)
Installed components:
• VCM Agent
• Package Studio
• Software Repository
• Package Manager (optional)
Software Repository A
Software Repository B

Install the Software Provisioning Components

The software provisioning components are installed on the VCM Collector by default. VMware recommends that you install the Software Repository for Windows and the VMware vCenter Configuration Manager Package Studio on a machine other than the Collector.

The software provisioning components should be installed on machines with these relationships:

- **Software Repository for Windows:** Installed on at least one Windows machine in your environment, and installed on the same machine with Package Studio. Install the repository before installing Package Studio.
- **VMware vCenter Configuration Manager Package Studio:** Installed on the same machine as your software repository.
- **Package Manager:** Installed on all Windows machines on which you are managing software provisioning.

To uninstall the applications using a script at a later date, you should save a copy of each of the .msi files in an archive location. To uninstall using the .msi, you must have the same version used to install the application.

Procedure

1. "Install Software Repository for Windows" on page 219

   The Software Repository for Windows and the VMware vCenter Configuration Manager Package Studio should be installed on the same machine. Installing the repository installs the Repository folders and subfolders, and configures the virtual directory. The virtual directory is used by Package Manager to access the repository.

2. "Install Package Studio" on page 220

   You must install the VMware vCenter Configuration Manager Package Studio and the repository on the same machine. The process installs the application files and specifies the repository to which Package Studio will publish packages.

3. "Install Package Manager on Managed Machines" on page 222

   The Package Manager, which installed on the target machines, manages the installation of the software packages. It does not contain the software packages, only pointers to the packages in the repository sources of which it is aware.

Install Software Repository for Windows

The Software Repository for Windows and the VMware vCenter Configuration Manager Package Studio should be installed on the same machine. Installing the repository installs the Repository folders and subfolders, and configures the virtual directory. The virtual directory is used by Package Manager to access the repository.

Prerequisites

- Verify that the target machine meets the supported hardware, operating system, and software requirements. See the *VCM Installation Guide* for currently supported platforms and requirements.
- Ensure that you have access to the `Repository.msi`, which is available on the VMware Web site or in the vCenter Configuration Manager application files. The default location in the VCM application files is `C:\Program Files (x86)\VMware\VCM\AgentFiles\Products`.

Procedure

1. Double-click `Repository.msi`.
2. On the Welcome page, click **Next**.
3. Review the license agreement, select the appropriate options to continue, and click **Next**.
4. On the Installation Folder page, use the default path or click **Change** to modify the path, and click **Next**.
5. On the Virtual Directory page, use the default name or type a new name in the text box, and click **Next**.
6. On the Ready to Install page, click **Install**.
7. When the Setup Completes page appears, click **Finish**.

The repository and the virtual directory are added to the locations specified during installation. The default location for the repository is `C:\Program Files\VMware\VCM\Tools\Repository` (on 32-bit machines) or `C:\Program Files (x86)\VMware\VCM\Tools\Repository` (on 64-bit machines). The default virtual directory SoftwareRepository is added to **Internet Information Services (IIS) > Web Sites > Default Web Site**.

Manually Uninstall the Repository

Using the command line syntax, you can run an unattended uninstall the software repository.

Prerequisites

To uninstall the application, use the same version of the `Repository.msi` that was used to install the application.

Procedure

1. Copy the `Repository.msi` to the machine on which you are uninstalling the application or point to the file in a shared directory.
2. Run the .msi file using the following command line syntax:

```
msiexec /x [path]\Repository.msi /l*v %temp%\Repository.log
```

Install Package Studio

You must install the VMware vCenter Configuration Manager Package Studio and the repository on the same machine. The process installs the application files and specifies the repository to which Package Studio will publish packages.

Prerequisites

- Verify that the target machine meets the supported hardware, operating system, and software requirements. See the *VCM Installation Guide* for currently supported platforms and requirements.
- Ensure you have access to the `PackageStudio.msi`, which is available on the VMware Web site or in the vCenter Configuration Manager application files. The default location in the VCM application files is `C:\Program Files (x86)\VMware\VCM\AgentFiles\Products`.
- Verify that the Software Repository for Windows is installed. Installing the repository before installing Package Studio reduces the manual configuration steps.

Procedure

1. Double-click `PackageStudio.msi`.
2. On the Welcome page, click **Next**.
3. Review the license agreement, select the appropriate options to continue, and click **Next**.
4. On the Installation Folder page, use the default path or click **Change** to modify the path, and click **Next**.
5. On the Repository Root Folder page, verify the path is to your installed repository files.

   If the path is not accurate, click **Change**. When the path is correct, click **Next**.
6. On the Ready to Install page, click **Install**.
7. On the Setup Complete page, click **Finish**.

The Package Studio is installed to the location specified during installation. The default location is `C:\Program Files\VMware\VCM\Tools\Package Studio` (on 32-bit machines) or `C:\Program Files (x86)\VMware\VCM\Tools\Package Studio` (on 64-bit machines).

To start Package Studio, click **Start** and select **All Programs > VMware vCenter Configuration Manager > Tools > Package Studio**, or open the Package Studio folder and double-click **PackageStudio.exe**.

Install Package Studio Using Unattended .MSI

The manual installation process installs the application files and specifies the repository to which Package Studio will publish packages.

Prerequisites

- Verify that the target machine meets the supported hardware, operating system, and software requirements. See the *VCM Installation Guide* for currently supported platforms and requirements.
- Ensure you have access to the `PackageStudio.msi`, which is available on the VMware Web site or in the vCenter Configuration Manager application files. The default location in the VCM application files is `C:\Program Files (x86)\VMware\VCM\AgentFiles\Products`.
- Verify that the Software Repository for Windows is installed. Installing the repository before installing Package Studio reduces the manual configuration steps.

Procedure

1. On your Collector, go to `C:\Program Files (x86)\VMware\VCM\AgentFiles\Products`.
2. Locate the `PackageStudio.msi` file and copy it to the target machine or a share location.
3. On the target machine, run the .msi file using the following command line syntax.

   ```
   msiexec /i [path]\PackageStudio.msi /qn /l*v %temp%\PackageStudio.log
   ```

   You can add the following arguments if you want to specify locations other than the default directories:

   `REPOSITORY_ROOT=C:\Program Files (x86)\VMware\VCM\Tools\Repository\` (Defaults to this or uses the Repository's value if it is already installed)

   `PACKAGESTUDIO_DIR="C:\Program Files (x86)\VMware\VCM\Tools\Package Studio\"` (defaults to this path)

The Package Studio is installed to the location specified during installation. The default location is `C:\Program Files\VMware\VCM\Tools\Package Studio` (on 32-bit machines) or `C:\Program Files (x86)\VMware\VCM\Tools\Package Studio` (on 64-bit machines).

To start Package Studio, click **Start** and select **All Programs > VMware vCenter Configuration Manager > Tools > Package Studio**, or open the Package Studio folder and double-click **PackageStudio.exe**.

Manually Uninstall Package Studio

Use the following script to run an unattended uninstall the Package Manager.

Prerequisites

To uninstall the application, you must use the version of the `PackageStudio.msi` that was used to install the application.

Procedure

1. Copy the `PackageStudio.msi` to the machine on which you are uninstalling the application or a shared location.
2. Run the installation file using the following command line syntax:

   ```
   msiexec /x [path]\PackageStudio.msi /l*v %temp%\PackageStudio.log
   ```

When Package Studio is uninstalled from a machine, the locally saved projects and `.crate` files remain on the machine, allowing you to copy them to another machine or to delete them manually if they are not needed.

Install Package Manager on Managed Machines

The Package Manager, which installed on the target machines, manages the installation of the software packages. It does not contain the software packages, only pointers to the packages in the repository sources of which it is aware. When directed to install, the package is copied from the repository to the cratecache folder on the target machines. Package Manager upzips the files to the %TMP% directory and runs the configured installation.

The Package Manager is installed on target machines when the 5.3 VCM Agent or later is installed from the Collector.

When a Remove Package action is sent to Package Manager, it checks first for the package in the cratecache. If it is not found, it then checks the repository sources for the package, and again copies it to the target machine's `cratecache folder` where it unzips the files. The configured uninstall files may be run from the zip directory.

Installing the VCM Agent

If you are preparing to use software provisioning on machines not previously managed in VCM, you must first install the VCM Agent. See "Install the VCM Windows Agent on Your Windows Machines" on page 91 for complete instructions. When you install the VCM Agent from the Collector, the installation includes the agent extensions for provisioning and the Package Manager for Windows. If you manually install the Agent using the MSI or EXE, you must manually install the Package Manager and the necessary agent extensions. See the online Help.

This default action is based on the settings in **Administration > Settings > General Settings > Installer**.

Prerequisites

Verify that the target machine meets the supported hardware, operating system, and software requirements. See the *VCM Installation Guide* for currently supported platforms and requirements.

Verifying the Installation of the Agent Extensions for Provisioning

If you do not know whether the machines are ready to use provisioning, you can verify the version of the Agent Extensions for Provisioning. The Agent Extensions for Provisioning include the Package Manager.

1. Select **Administration > Machines Manager > Licensed Machines > Licensed Windows Machines**.
2. In the data grid, locate the machines on which you are verifying the existence of the necessary Agent Extensions and verify that the Agent Ext. For Prov. Version column contains a value of 5.3 or later.

   If it does not, you need to either install or upgrade the VCM Agent.

Upgrading the VCM Agent

If an earlier VCM Agent is installed on your machines, you will need to upgrade to the latest Agent. See Upgrade Agent in the online Help.

Using Package Studio to Create Software Packages and Publish to Repositories

Package Studio is the application used to build software packages for installation on target Windows servers and workstations.

Windows packages can include in-house and commercial software installation files, including .msi, .exe, VBScripts, python, PowerShell.

To add a software installer to a package, it must be able to install and uninstall unmanned or quietly using command line options, response files, or other similar methods.

Creating Packages

You use Package Studio to create packages, including the installation files and the required metadata. When the package is ready for use, you publish it to a repository. The procedure here is only a general process. See the Package Studio online Help or the *VCM Software Provisioning Installation and User's Guide* for the detailed procedures.

Procedure

1. Start the VMware vCenter Configuration Manager Package Studio. Select **Start > All Programs All > VMware vCenter Configuration Manager > Tools > Package Studio**.

   NOTE If you are running Package Studio on the Collector or a Windows 2008 Server, you must run the application as administrator. See "Run Package Studio as Administrator" on page 224 for more information.

2. Click **Manage Packages**. Configure the package contents based on the options on the following tabs:

a. Click **Properties** and type a Name, Version, Description, and select the Architecture. These fields are required. You have the option to update the other fields, depending on you requirements.

   Configuring the package with Depends, Conflicts, Provides, and adding and configuring the installation and removal files.

b. Click **Files** and import the installation files, add pre-command files, configure the commands and arguments, and add post-command files.

c. Click **Save** to save the setting and files as a Project (*.prj).

d. Click **Generate** to save the project as a package (*.crate).

3. Click **Package Signing** and sign the package with a signing certificate.

   a. Click **Open** to select a package (*.crate file).

   b. Click **Sign** and select a certificate from the certificate store or from a file.

4. Click **Manage Repositories** and select the platforms and sections to which you are publishing the package.

   a. Click **Add Platforms** to add a platform.

   b. Select a platform, and then click **Add Sections**.

   c. Select a section, and then click **Publish Package**.

   d. Select the package (.crate) and click **Open**.

   e. (Optional) Select additional platforms and sections to which to publish the package.

   f. Click **Publish**. The package is published to the software repository.

5. Click **External Software** and add externally managed software, especially any packages specified as depends or conflicts in any of your packages.

   a. Click **New External Package** and replace the text with the name you will use as an external software package name.

   b. Type a version number in the Version text box.

   c. Select the **Architecture** in the drop-down menu.

   d. Click **Select Attribute Name** and select a registry property or WMI attribute in the drop-down menu.

   e. Add attributes.

   f. To save a copy locally, click **Save** .

   g. Click **Publish External SW** to publish to the repository.

Run Package Studio as Administrator

The enhanced security on Windows 2008 Server requires you to run Package Studio as an administrator. If you do not, you will not be able to publish packages to the repository.

NOTE You do not need to run Package Studio as administrator if your repositories were configured on non-UAC protected paths or when you are running Package Studio and the repositories on machines other than a Windows 2008 Server.

Procedure

1. On a Windows 2008 machines, select **Start > All Programs > VMware vCenter Configuration Manager > Tools**.
2. Right-click **Package Studio** and select **Properties**.
3. Click the **Compatibility** tab.
4. In the Privilege Level area, select **Run this program as an administrator** and click **Apply**.
5. Click **OK**.
6. Select **Start > All Programs > VMware vCenter Configuration Manager > Tools > Package Studio**.
7. On the User Account Control dialog box, click **Yes**.

Using VCM Software Provisioning for Windows

Using VCM Software Provisioning, you collect and view Repository and Package Manager data, and then install or remove packages on target machines.

Prerequisites

Software packages are created and published to the repository. See "Creating Packages" on page 223.

Procedure

1. "Collect Package Manager Information from Machines" on page 225

   To view information about packages and Package Managers in VCM, you must collect Package Manager data from managed machines.

2. "Collect Software Repository Data" on page 226

   Collect the repository data to identify which software packages are in which repositories. From the collected information, you can determine which repositories to assign to machines based on the available packages.

3. "Add Repository Sources to Package Managers" on page 227

   Sources are the sections in the repository from which the Package Manager will be able to download and install packages.

4. "Install Packages" on page 228

   The process of installing packages includes identifying and processing dependencies and conflicts; running any specified prescripts; running the installation using any specified command arguments; and running any specified post-scripts.

Collect Package Manager Information from Machines

To view information about packages and Package Managers in VCM, you must collect Package Manager data from managed machines.

Regularly collect Package Manager data to determine if your machines are remaining current with the necessary software packages.

Prerequisites

- Package Manager is installed on the target machines. Package Manager is installed when you install the VCM 5.3 Agent or later. See "Install Package Manager on Managed Machines" on page 222.
- Verify that you created software provisioning packages using VMware vCenter Configuration Manager Package Studio and published the packages to the repositories. See "Creating Packages" on page 223.

Procedure

1. Click **Collect**.
2. Select **Machine Data**.
3. Click **OK**.
4. On the Machines page, verify that the **Selected** pane displays all the machines from which you are collecting package manager data and click **Next**.
5. On the Data Types page, expand **Windows**, select **Software Provisioning - Package Managers**, and click **Next**.
6. On the Confirmation page, review the information, resolve any conflicts, and click **Finish**.

   You can monitor the process in the **Jobs Manager**. See "Viewing Provisioning Jobs in the Job Manager" on page 230.

What to do next

- When the collection is finished, view the collected data. Click **Console** and select **Windows tab > Operating System > Software Provisioning > Package Managers**. The data grid displays the packages and their current status.
- Collect repository data from the Software Repository for Windows. See "Collect Software Repository Data" on page 226.

Collect Software Repository Data

Collect the repository data to identify which software packages are in which repositories. From the collected information, you can determine which repositories to assign to machines based on the available packages.

To better manage your repository machines, create a machine group containing all the machines on which the software repository is installed.

Prerequisites

Verify that you created software provisioning packages using VMware vCenter Configuration Manager Package Studio and published the packages to the repositories. See "Creating Packages" on page 223.

Procedure

1. Click **Collect**.
2. Select **Machine Data**.
3. Click **OK**.
4. On the **Machines** page, verify that the **Selected** pane displays all the machines from which you are collecting repository data and click **Next**.

5. On the **Data Types** page, expand **Windows**, and select **Software Provisioning - Repositories**, and click **Next**.
6. On the Confirmation page, review the information, resolve any conflicts, and click **Finish**.

   You can monitor the process in the **Jobs Manager**. See "Viewing Provisioning Jobs in the Job Manager" on page 230.

What to do next

- When the collection is finished, view the collected data. Click **Console** and select **Windows tab > Operating System > Software Provisioning > Repositories**. The data grid displays the packages in the repositories.
- Add the repositories to the Package Manager. See "Add Repository Sources to Package Managers" on page 227.

Add Repository Sources to Package Managers

Sources are the sections in the repository from which the Package Manager will be able to download and install packages.

Adding a source gives the Package Manager on the selected machines access to the packages available in specified section. The sources are numbered in priority order. When you add a new one, you can specify whether to add it to the beginning or to the end of the list. You can also remove sources.

Prerequisites

- Verify that you collected Package Manager data from the target machines. See "Collect Package Manager Information from Machines" on page 225.
- Verify that you collected repository data from software repository. See "Collect Software Repository Data" on page 226

Procedure

1. Click **Console**.
2. Select **Windows tab > Operating System > Software Provisioning > Package Managers**.
3. Select one or more machines, and click **Add Source**.
4. On the Select Machines page, verify that the machines displayed in the lower pane are the machines to which you want to add the source and click **Next**.
5. On the Enter or Select Source page, configure the options, and click **Next**.
   a. Select either **Add source at the beginning of existing source lists** or **Add source at the end of the existing source list**.
   b. Click **Browse Sources**.
   c. On the Browse Sources page, select one of the following in the Show Sources from drop-down menu.

- **Package Manager Source Lists:** Select this option if you have already added sources to at least one Package Manager and you want to add the source to other Package Managers. When you click **OK**, the selected source populates the Platform and Section on the Enter or Select Source page.
- **VCM Managed Repositories:** Select this option if the source has not yet been added to a Package Manager. When you return to the Enter or Select Source page, you must type the platform and section names in the appropriate text boxes.

d. Select the URI and click **OK**.

e. Verify that the Platform name and the Section name are exactly the names used in the repository.

6. On the Schedule page, select one of the scheduling options and configure as needed.
7. On the Confirmation page, review the information and click **Finish**.

The added source is displayed in the **Package Manager - Sources** data grid.

What to do next

Install software packages on target machines. See "Install Packages" on page 228.

Install Packages

The process of installing packages includes identifying and processing dependencies and conflicts; running any specified prescripts; running the installation using any specified command arguments; and running any specified post-scripts. You can also remove packages.

Prerequisites

Verify that you added the repository sources to the Package Managers. See "Add Repository Sources to Package Managers" on page 227.

Procedure

1. Click **Console**.
2. Select **Windows tab > Operating System > Software Provisioning > Package Managers**.
3. Click **Install Package**.
4. On the Select Machines page, verify that the machines displayed in the lower pane are the machines to which you want to install the package and click **Next**.
5. On the Select Package page, select the package to install.
6. Select one of the following version options.

Option	Description
Install Version	Installs the specified version. By default the operator equals the package selected in the list. However, you may select a different operator and type the version number in the text box.
Install latest available version on all platforms	Installs the latest version of the package available from the sources configured for the Package Manager.

7. Configure the Security Options and click **Next**.

Determine whether a package is installed or removed based on the state of the signature.

Option	Description
Install secure signed package only	The package must be signed and the public key of the signing certificate you used to sign the package is available on all the machines on which you are installing or removing the package.
Skip signature validation when installing a signed package	(Not Recommended) The package is installed or removed without attempting to verify the signature.
Allow unsigned package to be installed	(Not recommended) The package is installed or removed even if it is unsigned.

8. On the Schedule page, select one of the scheduling options and configure as needed.
9. On the Confirmation page, review the information, resolve any conflicts, and click **Finish**. You can monitor the process in the **Jobs Manager**. See "Viewing Provisioning Jobs in the Job Manager" on page 230.

The package is displayed as Installed in the **Package Manager - Packages** data grid.

Related Software Provisioning Actions

You can use the following management options in VCM when working with software provisioning.

Option	Description
Console	All Software Provisioning are available for auditing as part of Change Management. Click Console and select **Change Management > VCM Initiated** or **Non VCM Initiated** to view the data. Software Provisioning actions are not eligible for rollback through Change Management. Undo unwanted changes using Compliance enforcement remediation actions. See "Create Compliance Rules Containing Software Provisioning Remediation Actions" on page 231. Non VCM Initiated changes related to Software Provisioning include publishing packages to repositories from Package Studio and manually running command-line actions in Package Manager.
Compliance	You can create compliance rules based on software provisioning data types, and you can add provisioning remediation actions to rules. See "Create Compliance Rules Based on Software Provisioning Data" on page 230 and "Create Compliance Rules Containing Software Provisioning Remediation Actions" on page 231.
Reports	You can run reports on collected Software Provisioning data. Click Reports and select **Machine Group Reports > Software Provisioning** to run the default reports, or you can create your own.

Option	Description
Administration	Displays current jobs running, and job history. Use the job history when troubleshooting the processing of a job. See "Viewing Provisioning Jobs in the Job Manager" on page 230. Define user access rules and roles to specify what level of access users have to the Software Provisioning data and actions in VCM. Click Administration and select **User Rules and Roles > User Manager > VCM Access** to configure the Access Rules and Roles.

Viewing Provisioning Jobs in the Job Manager

The Jobs Manager tells you the state of a currently running Provisioning job, including the success or failure of a job, either collecting data from machines or installing, updating, or removing packages from machines.

The currently running provisioning jobs are visible in the following locations:

- Jobs button. Located on the portal toolbar.
- Administration slider. Select **Administration > Job Manager > Running**.

Job history is available in **Administration > Job Manager > Other Jobs**. The provisioning related job names include the following types of jobs:

- Change Request: Add Source
- Change Request: Remove Source
- Change Request: Install Package
- Change Request: Remove Package

Create Compliance Rules Based on Software Provisioning Data

A Compliance rule based on software provisioning data detects any packages or sources that are out of compliance. You can configure remediation actions to bring the machines back into compliance.

In this example the Compliance rule checks whether the source, where the values are platform=Any and section=Release, was added to selected Package Managers as a source. If not, then add the repository source to the machines where the rule fails.

Procedure

1. Click **Compliance**.
2. Select **Machine Group Compliance > Rule Groups**.
3. Expand your rule group and select **Rules**.
4. On the Rules data grid, click **Add**.
5. Type a Name and Description for your rule and click **Next**.
6. On the Data Type page, expand **Windows** and select the data type on which you are basing the rule and click **Next**.

   In this example, select **Software Provisioning - Package Managers - Sources**.
7. On the Rule Type page, select **Conditional (if/then)** and click **Next**.
8. On the Conditional Data page, configure the options.

a. In the IF area, click **Add**.

b. Select `Source Repository URI = YourRepository`.

c. Select **Must Exist**.

d. In the THEN area, click **Add** and select `Platform = Any` and `Section = Release`.

e. Click **Next**.

9. On the Options page, configure the settings.

a. Select a Severity in the drop-down menu.

b. Select **Make available for enforcement where possible**.

c. Select **Software Provisioning action**.

d. Select **Add Source** in the drop-down menu and click **Define Action**.

e. On the Software Provisioning Compliance Remediation page, select **Add source to the beginning of existing source list**.

f. Click **Browse Sources** and select the repository URI where the Platform=Any and Section=Release exist, and click **OK**.

The Platform and Section update with Any and Release respectively.

g. Click **OK**.

h. Click **Next**.

10. On the Collection filters page, select the **Provisioning - Package Managers** collection filter and click **Next**.

11. On the Important page, review the information and click **Finish** to save your rule.

What to do next

Add the rule to your template. When the Compliance Template is run, it checks the target machines to determine if the repository source is added as a source. If it is not, the source is added to the machines Package Manager.

Create Compliance Rules Containing Software Provisioning Remediation Actions

When configuring a Compliance rule, you can configure the rule to perform a remediation based on a software provisioning action such as Install Package, Remove Package, Add Source, or Remove Source.

In this procedure, the example is to determines whether a software application named XSoftware is installed. If the software is installed correctly, a service named XService should be running. Configure a Compliance rule to determine if XService service is running. If it is not running, install the XSoftware package.

Procedure

1. Click **Compliance**.
2. Select **Machine Group Compliance > Rule Groups**.
3. Expand your rule group and select **Rules**.
4. On the Rules data grid, click **Add**.
5. On the Rule and Name page, type a Name and Description for your rule and click **Next**.

6. On the Data Type page, expand Windows, select the data type on which you are basing the rule, and click **Next**.

   The data type does not need to be software based. In this example, select **Services**.

7. On the Rule Type for Services page, select **Conditional (if/then)** and click **Next**.
8. On the Conditional Data properties page, configure the options and click **Next**.
   a. In the IF section, click **Add**.
   b. Select `Services Name = XService`.
   c. Select **Must Exist**.
   d. In the THEN section, click **Add**.
   e. Select `State = Running`.
9. On the Options page, configure the options.
   a. Select a **Severity** in the drop-down menu.
   b. Select **Make available for enforcement where possible**.
   c. Select **Software Provisioning action**.
   d. Select **Install Package** in the drop-down menu, and click **Define Action**.
   e. On the Software Provisioning Compliance Remediation page select the `XSoftware` package to install if the rule you are configuring fails.
   f. Configure the version options to use the selected version, specify a different version, or install the latest version.
   g. Specify the Security Options.

      Determine whether a package is installed or removed based on the state of the signature.

Option	Description
Install secure signed package only	The package must be signed and the public key of the signing certificate you used to sign the package is available on all the machines on which you are installing or removing the package.
Skip signature validation when installing a signed package	(Not Recommended) The package is installed or removed without attempting to verify the signature.
Allow unsigned package to be installed	(Not recommended) The package is installed or removed even if it is unsigned.

   h. Click **OK** and click **Next**.
10. On the Collection filters page, select the `Services` collection filter and click **Next**.
11. On the Important page, review the information and click **Finish** to save your rule.

What to do next

Add the rule to your compliance template. When the template is run, if the check for XService running fails, the XSoftware package is installed.

Configuring Active Directory Environments

13

VCM for Active Directory collects Active Directory objects across domains and forests, and displays them through a single console. The information is consolidated and organized under the Active Directory slider, allowing you to view your Active Directory structure, troubleshoot issues, detect change, and ensure compliance.

You can filter, sort, and group Active Directory data to pinpoint the specific area of interest. You can also view a subset of your Active Directory (a forest, domain, or specific organizational unit branch) by setting the Active Directory location in the AD Location field near the top of VCM. Dashboards display high level information in graphical form, alerts notify you about problems or misconfigurations, and change management tracks changes to the Active Directory objects or configuration by data type.

This chapter includes the following topics:

Configure Domain Controllers 233
Configure VCM for Active Directory as an Additional Product 239
Collect Active Directory Data 242
Active Directory Collection Results 242

Configure Domain Controllers

To manage your Active Directory environment, you must verify domains and accounts, discover and license domain controllers, install the VCM Agent, and collect data from the domain controllers.

Procedure

1. "Verify Available Domains" on page 234

   Allow VCM access to each domain so that the VCM Collector can interact with the domain controllers in your environment.

2. "Check the Network Authority Account" on page 234

   Verify that at least one domain account with administrator privileges is available to act as a network authority account for VCM.

3. "Assign Network Authority Accounts" on page 235

   Select and assign the network authority account that you identified for VCM access to the domain controllers.

4. "Discover Domain Controllers" on page 235

   In your network, identify the domain controllers that you are managing with VCM.

5. "License Domain Controllers" on page 236

   To manage domain controllers, you must license them in VCM.

6. "Install the VCM Windows Agent on Your Domain Controllers" on page 237

   Install the VCM Windows Agent on each domain controller so that you can collect data and manage the virtual or physical machines.

7. "Collect Domain Controller Data" on page 238

   Start managing the domain controllers by performing an initial collection, which adds domain controller data to VCM.

Continuous domain controller management is based on the latest data that you collect from target machines. You can view data and run actions, such as reports or compliance, based on the collected data. See "Windows Collection Results" on page 94.

Verify Available Domains

Allow VCM access to each domain so that the VCM Collector can interact with the domain controllers in your environment.

During installation, VCM discovered all domains to which the network authority account had access. If the domain controllers belong to a domain that is not listed, you must add that domain manually.

Prerequisites

Verify that you have the fully-qualified names of the domains to manage.

Procedure

1. Click **Administration**.
2. Select **Settings > Network Authority > Available Domains**.
3. If the domain does not appear Available Domains view and have a **Domain Type** of Active Directory, add the domain.
   a. Click **Add**.
   b. Type the domain name and select the domain type as **AD**.
   c. Click **OK**.
4. Verify that the domain appears in the data grid.

What to do next

Verify that a network authority account is available and create other necessary domain accounts. See "Check the Network Authority Account" on page 234.

Check the Network Authority Account

Verify that at least one domain account with administrator privileges is available to act as a network authority account for VCM.

VCM network authority accounts must have administrator privileges on each domain to be managed in the organization. Although you specified an initial default network authority account when you installed VCM, you can add different administrator accounts if you do not assign the default account.

Prerequisites

Verify the presence of domains. See "Verify Available Domains" on page 234.

Procedure

1. Click **Administration**.
2. Select **Settings > Network Authority > Available Accounts**.
3. To add a new domain account, click **Add**.
4. Type the domain name, user name, and password, and click **Next**.
5. Click **Finish** to add the account.

What to do next

Assign the network authority account to the domain so that VCM can access the domain controllers in the domain. See "Assign Network Authority Accounts" on page 235.

Assign Network Authority Accounts

Select and assign the network authority account that you identified for VCM access to the domain controllers.

Assign an account with administrator privileges on the domain.

Prerequisites

Verify or add the necessary network authority account. See "Check the Network Authority Account" on page 234.

Procedure

You must perform the following steps twice, once for NetBios and once for Active Directory.

1. Click **Administration**.
2. Select **Settings > Network Authority > Assigned Accounts > By Domain > NetBios**.
3. Select an assigned account.
4. Click **Edit Assigned Accounts**.
5. Select the account to receive authority to the domain and click **Next**.
6. Confirm the accounts to include in the authority list for the domain and click **Finish**.

What to do next

- Repeat the preceding assignment steps, and select Active Directory in step 2.
- Discover the domain controllers in your environment. See "Discover Domain Controllers" on page 235.

Discover Domain Controllers

In your network, identify the domain controllers that you are managing with VCM.

To discover the available domain controllers, VCM uses general discovery rules to identify many Windows machines or uses specific discovery rules to identify particular Windows machines.

The time required to perform an initial discovery depends on the size and composition of your network. If all domain controllers are not available during initial discovery, such as systems that are disconnected from the network, the first discovery will not find all domain controllers. If the discovery does not identify all domain controllers, you might need to run additional discoveries after the other domain controllers become available.

NOTE You can use the Discovered Machines Import Tool (DMIT), which imports machines discovered by the Network Mapper (Nmap), to import many physical and virtual machines at one time into the VCM database. Download DMIT from the VMware Web site.

Prerequisites

Assign a Network Authority Account that VCM can use for access. See "Assign Network Authority Accounts" on page 235.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Discovery Rules**.
3. Click **Add** to create a discovery rule.
4. Type a name and description and click **Next**.
5. Select **By Browse List** and click **Next**.
6. Select **Only discover machines in the Browse List that match these criteria**.
7. Select and type the following filter parameters.

   Where **Domain Controller Type** **< >** " (two single quotes, no space)
8. Click **Next**.
9. Click **Yes** and click **Finish**.
10. On the toolbar, click **Jobs** to track current discovery job status.

What to do next

- Verify that the jobs finished running. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.
- Verify that the domain controllers are available. Click **Administration** and select **Machines Manager > Available Machines**.
- License the domain controllers in your environment. See "License Domain Controllers" on page 236.

License Domain Controllers

To manage domain controllers, you must license them in VCM.

The number of discovered domain controllers might exceed the number of your available licenses. If that happens, the number available goes negative and appears in red to indicate that you do not have enough licenses.

For servers and workstations, exceeding the limit on your license key produces warnings but does not restrict VCM operation. License key counts that are over the limit are recorded and maintained for auditing purposes. Suite license keys support unlimited licenses, provided that the suite edition includes VCM and the component that you are managing is part of the suite. If a component is not part of the suite, it counts against the nonsuite server or workstation key.

Prerequisites

Verify that the domain controllers you license are listed with a machine type of workstation or server in the Available Machines node. If the discovered or added type is not workstation or server, VCM cannot license the machines.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Available Machines**.
3. Select the domain controllers to license.
4. Click **License**.
5. Verify that the domain controllers to license appear in the Selected list.

   Use the arrows to move the domain controllers.
6. Click **Next** to view your Product License Details.

   The licensed domain controller count increases by the number of licensed machines.
7. Click **Next**.

   VCM confirms that the licenses you requested will be applied to the selected domain controllers.
8. Click **Finish**.

What to do next

Install the VCM Windows Agent. See "Install the VCM Windows Agent on Your Domain Controllers" on page 237.

Install the VCM Windows Agent on Your Domain Controllers

Install the VCM Windows Agent on each domain controller so that you can collect data and manage the virtual or physical machines.

Before you can collect data from domain controllers, you must install the VCM Windows Agent on the licensed domain controllers in your environment to enable communication between the Collector and the target machines.

Standardized Windows configurations such as Federal Desktop Core Configuration (FDCC) or United States Government Configuration Baseline (USGCB) include strict security group policy settings. The **Windows Firewall: Do not Allow Exceptions** group policy configures Windows Firewall to block all unsolicited incoming messages, including configured exceptions. This setting overrides all configured exceptions. For VCM to communicate properly with the VCM Agent on managed machines in strict, secure environments, disable the **Windows Firewall: Do not Allow Exceptions** group policy on the managed machines. For more information, see support.microsoft.com.

Prerequisites

- License the domain controllers on which you install the Agent. See "License Domain Controllers" on page 236.
- Verify that you know the communication protocols and ports that are used by the Collector and the Agents.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed Windows Machines**.
3. In the data grid, select one or more domain controllers on which to install the Agent and click **Install**.
4. On the Machines page, verify that the target machines appear in the Selected list and click **Next**.
5. On the Install Options page, select the default installation options and click **Next**.
6. On the Schedule page, select **Run Action now** and click **Next**.

   You can schedule subsequent Agent installations to run later.
7. Review the summary information and click **Finish**.

What to do next

- Verify that the jobs finished running. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.
- Collect Windows data from VCM managed domain controllers in your environment. See "Collect Domain Controller Data" on page 238.

Collect Domain Controller Data

Start managing the domain controllers by performing an initial collection, which adds domain controller data to VCM.

Use the default filter set to collect a general view of the domain controllers in your environment. The first time that you use the default filter to collect data, the Windows Agent returns all of the data specified in the filter and stores the data in the VCM database. All subsequent collections will return a delta against the data previously collected.

A delta collection includes only the differences between the data on the target machine and the data stored in the VCM database. If you need a full collection, you can specify that VCM collect all data again. A full collection can take a significant amount of time depending on the number of VCM managed domain controllers from which you are collecting.

When you perform a full collection from your entire environment, run the collection during nonworking hours so that users do not notice any performance impact on managed machines. After the initial collection is finished, subsequent delta collections will most likely not impact performance.

Prerequisites

- To collect data from Windows XP SP2 or Vista machines that use DCOM communication, you must enable ICMP pings in the firewall settings or disable ICMP pings in VCM.
- Verify that DCOM is enabled on the managed machine. Run `dcomcnfg` and select **Enable Distributed COM on this computer**.

Procedure

1. On the VCM toolbar, click **Collect**.
2. On the Collection Type page, select and click **OK**.
3. On the Machines page, select the domain controllers from which to collect data and click **Next**.

   To move all visible domain controllers to the selection window, use the double arrow.
4. Select the **Do not limit collection to deltas** check box.

   This option ensures that a full collection occurs during the initial set up of VCM for Active Directory.
5. On the Data Types page, configure the collection and click **Next**.
   a. Expand Windows and select the data types.

      At a minimum, you must collect **Machines** data. If you are managing data using compliance, change, or running reports, you must collect the data types that are included in the other actions or that you want to view in the appropriate data grids.
   b. Select **Use default filters**.
6. On the Important page, resolve any conflicts and click **Finish**.
7. Click **Administration** and select **Job Manager > History > Instant Collections > Past 24 Hours** to determine if the collection finished.

   The amount of time the collection requires is determined by the number of machines and network connectivity.

What to do next

Add VCM for Active Directory. See "Configure VCM for Active Directory as an Additional Product" on page 239.

Configure VCM for Active Directory as an Additional Product

After VCM has discovered, licensed, and installed the Windows Agent on your domain controllers, configure VCM for Active Directory as an additional product. Configuring VCM for Active Directory provides the mechanism that allows VCM to manage the Active Directory forests and collect detailed schema information.

Procedure

1. "Install VCM for Active Directory on the Domain Controllers" on page 240

   To use VCM to collect Active Directory data from your environment, install VCM for Active Directory on your domain controllers.
2. "Run the Determine Forest Action" on page 240

   VCM for Active Directory requires a forest determination for all domain controllers so that it can proceed with schema and structure collection.
3. "Run the Domain Controller Setup Action" on page 241

   VCM for Active Directory collects your Active Directory schema and structure as part of the domain controller setup action.

Install VCM for Active Directory on the Domain Controllers

To use VCM to collect Active Directory data from your environment, install VCM for Active Directory on your domain controllers.

VCM for Active Directory will operate with only a single domain controller configured with VCM for Active Directory, which will serve as both the forest data source (FDS) and replication data source (RDS). However, to collect important nonreplicated attributes such as Last Logon, install VCM for Active Directory on as many domain controllers as possible.

Prerequisites

- Discover, license, and install the VCM Windows Agent on your domain controllers. See "Configure Domain Controllers" on page 233.
- Verify that the jobs finished running. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Additional Components > VCM for Active Directory**.
3. Click **Install**.
4. Move the domain controllers on which to install VCM for Active Directory to the lower pane.
5. Click **Next**.
6. Verify that **Run Action now** is selected and click **Finish**.

If you add future Active Directory machines to your environment, configure them with VCM for Active Directory by running the following installer.

```
Program Files (x86)\VMware\VCM\AgentFiles\ADProductInstall.exe
```

What to do next

Determine the Active Directory forest in your environment. See "Run the Determine Forest Action" on page 240.

Run the Determine Forest Action

VCM for Active Directory requires a forest determination for all domain controllers so that it can proceed with schema and structure collection.

Prerequisites

- Install VCM for Active Directory on your domain controllers. See "Install VCM for Active Directory on the Domain Controllers" on page 240.
- Verify that the jobs finished running. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Additional Components > VCM for Active Directory**.
3. Click **Determine Forest**.
4. Move the domain controllers on which to determine the forest to the lower pane.

   Determine the forest for all available domain controllers.
5. Click **Next**.
6. Click **Finish**.

What to do next

Run the domain controller setup action and identify your FDS and RDS. See "Run the Domain Controller Setup Action" on page 241.

Run the Domain Controller Setup Action

VCM for Active Directory collects your Active Directory schema and structure as part of the domain controller setup action.

During setup, you select a Forest Data Source (FDS) and Replication Data Source (RDS). Select machines that have reliable connections and availability. The same domain controller is allowed to serve as both FDS and RDS.

- **FDS**: VCM for Active Directory uses the FDS as a resource for all Forest-level information. You identify one FDS for each Forest.
- **RDS**: The RDS supplies all replicated data to VCM for Active Directory. You identify only one RDS for each domain so that collections on replicated attributes are performed only on a single domain controller. Other domain controllers that have VCM for Active Directory installed are accessed only during collection of nonreplicated attributes.

  If you change your RDS, VCM for Active Directory does not purge data collected from the old RDS. The data is refreshed when you run a new collection using the new RDS.

Prerequisites

- Use VCM for Active Directory to determine the Forest. See "Run the Determine Forest Action" on page 240.
- Verify that the jobs finished running. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Additional Components > VCM for Active Directory**.
3. Click **Setup DCs**.
4. Select an FDS for each forest and click **Next**.
5. Select an RDS for each domain and click **Next**.
6. Click **Finish**.

When the Setup DCs action finishes, VCM for Active Directory initiates the following jobs.

- Active Directory schema collection
- Active Directory specifier collection
- Active Directory structure collection

The information obtained from the third collection identifies the organizational unit (OU) structure that supports the use of VCM for Active Directory. To view information, click **Administration**, and select **Machines Manager > Additional Components > VCM for Active Directory**.

What to do next

Collect Active Directory data. See "Collect Active Directory Data " on page 242.

Collect Active Directory Data

Perform your first collection of Active Directory objects by launching the same collection wizard that you use for Windows, and Linux and UNIX collections. The first time you run an Active Directory collection, the Agent returns all objects and attributes from your selected Active Directory environment.

Prerequisites

- Install VCM for Active Directory. See "Configure VCM for Active Directory as an Additional Product" on page 239.
- Verify that jobs have finished by clicking **Administration** and selecting **Job Manager > History > Other Jobs > Past 24 Hours**.

Procedure

1. From the toolbar, click **Collect**.
2. On the Collection Type page, select **Active Directory** and click **OK**.
3. On the AD Collection Options page, click **Select Data Types to collect from these machines**.
4. To ensure that a full collection occurs, select the **Do not limit collection to deltas** check box and click **Next**.
5. On the Data Types page, click **Select All**.
6. Select the **Use default filters** option and click **Next**.
7. On the Location page, click the ellipsis button (...).
8. On the Select an AD Location page, expand the **Enterprise** tree, select an Active Directory Location, and click **OK**.
9. On the Location page, click **Next**.
10. Click **Finish**.

What to do next

Explore initial Active Directory collection results. See "Active Directory Collection Results" on page 242.

Active Directory Collection Results

After you collect the initial Active Directory data, explore the results under Active Directory, Reports, and Compliance.

Displayed information is only as current as the last time that you collected Active Directory data.

Option	Description
Active Directory Dashboard	Provides summary and day-to-day information about your Active Directory environment in a graphical format. ■ To view the dashboard, click **Active Directory** and select **Dashboards > Managed Objects**. Several Active Directory Dashboards are available.
Active Directory Object Summary	Provides summary information about your Active Directory environment in a textual format. ■ To view the summary reports, click **Active Directory** and select **Objects > *object-type***.
Active Directory Object Detail	Provides the detailed information behind the summary for your Active Directory environment. ■ To view the detailed information, click **Active Directory** and select **Objects > *object-type***. Click the **View data grid** button. From the data grid view, you can enable or disable the summary to view the details immediately.
Reports	Provides Active Directory information by running preconfigured or custom reports against the latest collected data. The time needed for a report to generate depends on the volume or complexity of the data requested. ■ To use the reporting options, click **Reports** and expand **Active Directory Reports**.
Compliance	Provides preconfigured Active Directory compliance rules and templates, which allow you to check the collected data against specific values. ■ To view Active Directory compliance rules, click **Compliance** and select **Active Directory Compliance > Rule Groups**. ■ To view Active Directory compliance templates, click **Compliance** and select **Active Directory Compliance > Templates**.

14 Configuring Remote Machines

The VCM Remote client is the communication and management mechanism that you use to manage mobile Windows machines as they connect to and disconnect from the network.

For Windows machines that are not continuously connected to the network, the VCM Remote client listens for network events indicating it has access to the VCM Remote-related components on the VCM Internet Information Services (IIS) server. Based on the configured settings, the Collector creates requests, such as a collection request, for the remote machine that has just become available online.

VCM Remote Management Workflow

To indicate the presence of the mobile Windows machine on your network, the VCM Remote client sends an HTML POST file over HTTP to a server-side component residing on the VCM Internet Information Services (IIS) server. Based on user-defined settings, the Collector auto-licenses the remote machine, installs or upgrades the VCM Windows Agent, and determines whether it should submit a collection job for that remote machine.

The Collector batches the requests and processes them at periodic intervals. This batch processing manages the problem of having 15,000 clients come online within a short time of one another and creating 15,000 individual requests.

Configuring VCM Remote Connection Types

The VCM Remote client accommodates three connection methods, including broadband, dial-up, and LAN, for Windows machines that do not have a continuous connection to the network.

To optimize the collection of the Windows machine data, you configure different collection filters for different connection types based on general bandwidth for each connection type.

- **Broadband:** DSL and cable connections can be 156Kb to more than 1Mb.
- **Dial-up:** A dial-up connection can be 56Kb or less.
- **LAN:** A local area connection to the network equal to or greater than 1Mb. A VPN connection might be available at LAN speeds but connected over the Internet.

For each connection type, you assign a customized collection filter set. For example, when a remote machine connects using a dial-up connection, you use a collection filter set that collects only key data compared to a filter set for LAN connections that collects more data from the target machines.

Using Certificates With VCM Remote

The use of certificates with VCM Remote ensures secure communication between VCM and the VCM Remote client when they are communicating outside your internal network.

The communication between the Collector and the VCM Remote client is secured using Transport Layer Security (TLS) certificates. You can use the VCM certificate or you can use an existing Enterprise certificate.

- **VCM Certificate:** A certificate generated during the installation of VCM. The VCM certificate is located on the Collector at `[install path]\VMware\VCM\CollectorData`. You must copy the `.pem` file to each target machine.
- **Enterprise Certificate:** A certificate already in the certificate store in your environment.

Determine the certificate that you are using to validate communication, either a VCM-generated or a Enterprise certificate in certificate store. By default, the installation of a Windows VCM Agent in HTTP mode adds the Collector's Enterprise Certificate to the certificate store of the client system. The VCM Remote client can also use this certificate.

After you install the VCM Remote client, the first time the remote machine connects the Collector network, it requests a Collector certificate. If the Collector certificate is trusted by the Enterprise certificate on the client, the Collector certificate is added to the client's certificate store.

Configure and Install the VCM Remote Client

You configure the VCM Remote client server-side communication settings and then install the client on target Windows machines. After it is installed, theVCM Remote client manages the communication with VCM when the remote machine is connected to the network.

Procedure

1. "Configure the VCM Remote Settings" on page 246

   You create custom filter sets for each communication method and configure the settings to ensure efficient on-going management of the mobile Windows machines managed using the VCM Remote client.

2. "Install the VCM Remote Client" on page 249

   You install the VCM Remote client on the target Windows machines that are not continuously connected to the network.

3. "Connect VCM Remote Client Machines to the Network" on page 256

   Connect your remote machine to the VCM-managed network to begin managing the machine. The VCM Remote client notifies VCM that the remote machine is on the network and it is processed based on VCM Remote settings and requires no user interaction.

When you configure Windows machines with the VCM Remote client, the client handles the communication when the remote machine connects to the network, but the machines are managed as Windows machines. See "VCM Remote Collection Results" on page 256.

Configure the VCM Remote Settings

You create custom filter sets for each communication method and configure the settings to ensure efficient on-going management of the mobile Windows machines managed using the VCM Remote client.

Procedure

1. "Create Custom Collection Filter Sets" on page 247

   You create custom collection filter sets for Dial-up, Broadband, or LAN connections to efficiently manage mobile machines using the VCM Remote client. To optimize results, create a different filter set for each connection type.

2. "Specify Custom Filter Sets in the VCM Remote Settings" on page 248

   VCM Remote supports three connection types: broadband, dial-up, and LAN. To optimize the collection of data, you must specify the collection filter set for each connection used in your environment.

3. "Specify Agent and Host File Settings" on page 248

   To ensure the VCM Remote client efficiently installs or upgrades the Agent and manages communication, you must configure the server settings on the Collector.

Create Custom Collection Filter Sets

You create custom collection filter sets for Dial-up, Broadband, or LAN connections to efficiently manage mobile machines using the VCM Remote client. To optimize results, create a different filter set for each connection type.

With filter sets based on connection type rather than using the default filter set, you can optimize collections based on the stability and speed of the connection. For example, an all encompassing collection is difficult to complete over a dial-up connection. To optimize the collection performance, create a dial-up filter set that is limited to a few high-importance data types and does not include the File System Uploads or Emergency Repair Disk data types.

Prerequisites

Review the purpose of the different connection types to understand what to include or exclude from your collection filter sets. See "Configuring VCM Remote Connection Types" on page 245.

Procedure

1. Click **Administration**.
2. Select **Collection Filters > Filter Sets**.
3. On the Collection Filter Sets data grid, click **Add Filter Set**.
4. On the Name and Description page, type a Name and Description.

   For example, use names similar to Remote Client - Broadband, Remote Client - LAN, and Remote Client - Dial-up.

5. Select **Filter Set** and click **Next**.
6. On the Filters page, select **Machine Based Filter Set**.
7. Select the filters to include in the filter set and click **Next**.
8. On the Conflicts page, resolve any data type conflicts and click **Next**.
9. On the Important page, review the summary information and click **Finish**.

What to do next

- Repeat the procedure for all the connection types for which you configure filter sets.
- Assign the filter sets to the appropriate VCM Remote settings. See "Specify Custom Filter Sets in the VCM Remote Settings" on page 248.

Specify Custom Filter Sets in the VCM Remote Settings

VCM Remote supports three connection types: broadband, dial-up, and LAN. To optimize the collection of data, you must specify the collection filter set for each connection used in your environment.

When a mobile Windows machine connects to the network using one of three connection types and the VCM Remote client indicates the presence of the machine, VCM determines the connection type and uses the collection filter specified for the connection when collecting data from the target machine. This method enables mobile VCM Remote client machines to connect using any of the connection types and to collect data using a filter set optimized for the connection type.

Prerequisites

Create VCM Remote collection filter sets, one for each connection type. See "Create Custom Collection Filter Sets" on page 247.

Procedure

1. Click **Administration**.
2. Select **Settings > General Settings > VCM Remote**.
3. On the VCM Remote Settings data grid, select each setting separately and click **Edit Settings**.
   - Name of the Collection Filter Set Remote will use for Broadband connections
   - Name of the Collection Filter Set Remote will use for Dialup connections
   - Name of the Collection Filter Set Remote will use for LAN connections
4. On the Edit Settings page, select the related filter set in the drop-down menu and click **Next**.
5. On the Important page, review the summary and click **Finish**.

What to do next

- Repeat the procedure for the other settings.
- Configure the Agent and host file settings. See "Specify Agent and Host File Settings" on page 248.

Specify Agent and Host File Settings

To ensure the VCM Remote client efficiently installs or upgrades the Agent and manages communication, you must configure the server settings on the Collector.

Procedure

1. Click **Administration**.
2. Select **Settings > General Settings > VCM Remote**.
3. On the VCM Remote Settings data grid, select each setting separately and click **Edit Settings**.

Option	Configuration
Should Remote automatically install an Agent to the client (if required)?	Click **Yes**. Allows VCM to install the Agent when contacted by the VCM Remote client the first time.
Should Remote automatically upgrade an Agent to the client (if required)?	Click **Yes**. Allows VCM to upgrade the Agent when contacted by the VCM Remote client.
Will IP Address of calling client be added to local host file?	Click **Yes**. Adds the IP address of the VCM Remote client to the host file to ensure that the remote client name is resolved and updated so that communication can begin.
Minutes to retain host File Entry	Type 30 or greater to specify 30 minutes or longer. Retains the IP address of the VCM Remote client in the host file for the set time to ensure that the remote client name is quickly resolved and updated during that time.

4. Configure the setting and click **Next**.
5. On the Important page, review the summary and click **Finish**.

What to do next

- Repeat procedure for the other settings on the VCM Remote Settings data grid.
- Install the VCM Remote client. See "Install the VCM Remote Client" on page 249.

Install the VCM Remote Client

You install the VCM Remote client on the target Windows machines that are not continuously connected to the network.

To install the VCM Remote client, use the method easiest to implement depending on your access to the target machines and the number of remote machines on which you are installing the client.

1. "Install the VCM Remote Client Manually" on page 250

   The manual installation of the VCM Remote client is a wizard-based process that you use when you have direct access to the target machines. This process is a useful way to install the client if you are creating an image to install on other machines.

2. "Install the VCM Remote Client Using a Command Line" on page 251

   You use the command line to install the VCM Remote client when you want to run an unattended installation using Group Policy or software provisioning.

3. "Install the VCM Remote Client Using Windows Remote Commands" on page 253

   You use the Windows remote commands to deploy the VCM Remote client to multiple machines in your environment. The VCM Agent must be installed on the target machines.

Install the VCM Remote Client Manually

The manual installation of the VCM Remote client is a wizard-based process that you use when you have direct access to the target machines. This process is a useful way to install the client if you are creating an image to install on other machines.

Prerequisites

Determine the certificate that you are using to validate communication between the client and the Collector. See "Using Certificates With VCM Remote" on page 246.

Procedure

1. On the target machine, create a folder and copy the files from the Collector to the target folder.

File	Description
`CM Remote Client.msi`	Located on the Collector at `[install path]\VMware\VCM\AgentFiles`.
`CM_Enterprise_Certificate_xxx.pem`	(Optional) Located on the Collector at `[install path]\VMware\VCM\CollectorData`. Copy the file if you do not have or are not using the Enterprise certificate located in the remote machine's certificate store.

2. On the target machine, double-click the `CM Remote Client.msi` file.
3. On the VCM Remote Client Setup page, click **Next**.
4. On the Installation Folder page, accept the default installation location or click **Change** to enter a different location, and click **Next**.

5. On the VCM Remote Client Information page, configure the options and click **Next**.

Option	Description
Collector Machine Name	Name of the Windows machine on which the VCM Collector and Microsoft IIS are installed.
Path to ASP Page	Path for the IIS default VCM Remote Web site. The <virtual directory name> must match the virtual directory name as it appears in the Collector's IIS. The default value is VCMRemote.

6. On the Select Certificates page, configure the certificate option that supports your environment and click **Next**.

Option	Description
Certificate File	Browse to the location of the VCM-generated `.pem` file you copied from the Collector.
Skip Certificate Deployment	Select the option to use the existing Enterprise certificate in the client certificate store.

7. On the Ready to install CM Remote Client page, click **Install**.
8. Click **Finish** when the installation is completed.

What to do next

Connect the remote machine to the network to ensure that VCM completes the installation process. See "Connect VCM Remote Client Machines to the Network" on page 256

Install the VCM Remote Client Using a Command Line

You use the command line to install the VCM Remote client when you want to run an unattended installation using Group Policy or software provisioning.

Prerequisites

Determine the certificate that you are using to validate communication between the client and the Collector. See "Using Certificates With VCM Remote" on page 246.

Procedure

1. On the target machine, create a folder and copy the files from the Collector to the target folder.

File	Description
CM Remote Client.msi	Located on the Collector at [install path]\VMware\VCM\AgentFiles.
CM_Enterprise_Certificate_xxx.pem	(Optional) Located on the Collector at [install path]\VMware\VCM\CollectorData. Copy the file if you do not have or are not using the Enterprise certificate located in the remote machine's certificate store.

2. At a command prompt, edit the installation command for you environment, and run the command.

   If the names and paths contain spaces, you must use double quotation marks.

```
msiexec.exe /qn /i "[path]\cm remote client.msi" COLLECTOR="YourCollectorName"
 PATHTOASP="VCMRemote/ecmremotehttp.asp" INSTALLDIR="c:\Program Files (x86)
\VMware\VCM Remote Client" CERTIFICATE_FILE="[path]
\YourEnterpriseCertificateName.pem" /l*v "[path\]filename.log"
```

Option	Description
/qn	No error messages appear during installation.
[path]\cm remote client.msi	Path to the CM Remote Client.msi on the target machine.
COLLECTOR=YourCollectorName	Replace <YourCollectorName> with the name of your VCM Collector.
PATHTOASP=VCMRemote/ecmremotehttp.asp	Path to the IIS Default Web Site virtual directory containing ecmremotehttp.asp.
INSTALLDIR:c:\Program Files (x86)\VCM\CM Remote Client	Path where you want the VCM Remote client files installed. The directory is created by the command.
CERTIFICATE_FILE=[path]\YourEnterprise CertificateName.pem	Certificate path and name on the target machine. If you are using an existing Enterprise certificate in the client certificate store, you use SKIP_CERTIFICATE_FILE=1 instead of CERTIFICATE_FILE=[path]\YourEnterpriseCertificateName.pem If the certificate does not exist in the store, any communication between the client and the Collector will fail.
/l*v [path\]filename.log	Error messages added to the log file in the specified path. If the path is not specified, the log file is saved in the directory from which the msiexec.exe was run.

What to do next

Connect the remote machine to the network to ensure that VCM completes the installation process. See "Connect VCM Remote Client Machines to the Network" on page 256

Install the VCM Remote Client Using Windows Remote Commands

You use the Windows remote commands to deploy the VCM Remote client to multiple machines in your environment. The VCM Agent must be installed on the target machines.

The script installs the VCM Remote client under the Windows directory rather than the Program Files directory. It is not necessary to create the install directory on the target machine before you run the script.

Prerequisites

- Verify that the Agent is installed on target machines. See "Configure Windows Machines" on page 87.
- Indentify the certificate you are using to validate communication between the client and the Collector. See "Using Certificates With VCM Remote" on page 246.

Procedure

1. On your Collector, copy `[install path]\Enterprise Configuration Manager\AgentFiles\CM Remote Client.msi` to `[install path]\Enterprise Configuration Manager\WebConsole\L1033\Files\Remote_Command_Files`.
2. On your Collector, copy `[install path]\Enterprise Configuration Manager\CollectorData\<YourEnterpriseCertificate>.pem` to `[install path]\Enterprise Configuration Manager\WebConsole\L1033\Files\Remote_Command_Files`.
3. In VCM, select **Console > Windows Remote Commands**.
4. On the data grid toolbar, click **Add**.
5. On the Name and Description page, type a unique name and description for the command, and click **Next**.
6. On the **Remote Command** page, configure the command.
   a. In the **Type** drop-down menu, select VBScript.
   b. In **Command Text** text box, copy and paste the script and modify it as specified in the script comments.

```
Call DoWork
'Copyright 1999-2010 VMware, Inc.
'Coded by Ryan L.
'Description: Installs VCM Remote ver. 2
'Modified 4/27/2008 - Stephen S. Included Certificate file options
'Modified 7/7/2010 - VCM
Dim sCollName, sInstallDir, sVirDir, sAddRemove, sCertFile, bInstallCert
Sub DoWork()
Set WshShell = CreateObject("WScript.Shell")
sCollName = "YourCollectorName" 'Name of your VCM Collector machine in
quotes
```

```
bInstallCert = 1 'If the value is 1, the Enterprise Certificate is
installed. If the value is set to 0, the installation of the certificate is
skipped and it is assumed that the certificate is already present. The
Remote Client will NOT function until the Enterprise Certificate is
installed as specified in Step 2

sCertFile = "EnterpriseCert" 'The filename of your enterprise certificate
(.pem file) as identified in Step 2

sVirDir = "VCMRemote/EcmRemoteHttp.asp" 'Where you replace CMRemote with
the IIS Default Web Site virtual directory containing the ECMRemoteHTTP.asp
 file

sInstallDir = WshShell.ExpandEnvironmentStrings("%windir%") & "\VMware\VCM
Remote Client" 'The installation directory on the TARGET machine

sAddRemove = 1 'Whether or not VCM remote should appear in the Add/Remove
programs List, should be 0 = hide, 1 = show

sMSIPackageName = "CM Remote Client.msi" 'Name of the MSI package that
installs VCM Remote Agent


CheckVars


If sAddRemove = 0 Then

AppToRun = "msiexec.exe /qn /i " & Chr(34) &
EcmAgtContext.JobDownloadDirectory & "\" & sMSIPackageName & Chr(34) & "
ALLUSERS=1 COLLECTOR=" & Chr(34) & sCollName & Chr(34) & " PATHTOASP=" &
Chr(34) & sVirDir & Chr(34) & " ARPSYSTEMCOMPONENT=" & sAddRemove & "
INSTALLDIR=" & Chr(34) & sInstallDir & Chr(34)

Else

AppToRun = "msiexec.exe /qn /i " & Chr(34) &
EcmAgtContext.JobDownloadDirectory & "\" & sMSIPackageName & Chr(34) & "
ALLUSERS=1 COLLECTOR=" & Chr(34) & sCollName & Chr(34) & " PATHTOASP=" &
Chr(34) & sVirDir & Chr(34) & " INSTALLDIR=" & Chr(34) & sInstallDir & Chr
(34)

End If

If bInstallCert = 1 Then

AppToRun = AppToRun & " CERTIFICATE_FILE=" & Chr(34) &
EcmAgtContext.JobDownloadDirectory & "\" & sCertFile & Chr(34)

Else

AppToRun = AppToRun & "SKIP_CERTIFICATE_FILE=1"

End If

EcmScriptRuntime.CmdExecute Chr(34) & AppToRun & Chr(34), 10000

End Sub
```

```
Sub CheckVars()
If sCollName = "" Then
WScript.Quit
Else
sCollName = Trim(sCollName)
End If

If sVirDir = "" Then
sVirDir = "vcmremote/ecmremotehttp.asp"
Else
sVirDir = Trim(sVirDir)
End If

If sInstallDir = "" Then
sInstallDir = "c:\vcm remote client"
Else
sInstallDir = Trim(sInstallDir)
End If

If sAddRemove <> 0 And sAddRemove <> 1 Then
sAddRemove = 1 'Set whether or not VCM Remote appears in the Add/Remove
programs list. 1=display, 0=do not display
End If

If sAddRemove = "" Then
sAddRemove = 1
End If

If IsNumeric(sAddRemove) = False Then
sAddRemove = 1
End If

sAddRemove = Trim(sAddRemove)
End Sub
```

c. Select the **Certain file(s) are required to be on the target machine for this remote command** check box.

d. Click **Next**.

7. On the Files page, move the `CM Remote Client.msi` file and the `.pem` file to the list on the right, and click **Next**.
8. On the Important page, review and summary and click **Finish**.

   VCM saves and adds the command to **Windows Remote Commands** list.
9. In the Windows Remote Commands data grid, select your VCM Remote installation remote command and click **Run**.
10. On the Machines page, select the Windows machines on which you are installing VCM Remote.
11. On the Schedule page, select when to run the installation and click **Next**.

    If you are running the installation command on many Windows machines at one time, schedule the installation for nonpeak network hours.
12. On the Important page, review the summary to verify the number of target machines and click **Finish**.

What to do next

- Verify that the installation is finished. To view the status of the Install CM Remote Client job, click **Administration** and select **Job Manager > History > Instant Collections**.
- Connect the remote machine to the network to ensure that VCM completes the installation process. See "Connect VCM Remote Client Machines to the Network" on page 256

Connect VCM Remote Client Machines to the Network

Connect your remote machine to the VCM-managed network to begin managing the machine. The VCM Remote client notifies VCM that the remote machine is on the network and it is processed based on VCM Remote settings and requires no user interaction.

Prerequisites

- Configure the VCM Remote server settings. See "Configure the VCM Remote Settings" on page 246.
- Install the VCM Remote client on target machines. See "Install the VCM Remote Client" on page 249.

Procedure

- Connect the remote machines to the VCM managed network.

  VCM Remote client sends a POST request to the VCM IIS server indicating its presence on the network. The Collector processes the request, auto-licenses the remote machine, installs or upgrades the VCM Windows Agent, and determines whether it should submit a collection job for that remote machine.

What to do next

Review the collected data. See "VCM Remote Collection Results" on page 256.

VCM Remote Collection Results

The VCM Remote client-specific data is limited to administrative details. All other data collected from the remote machine appears in VCM as Windows machine data. See "Windows Collection Results" on page 94.

The displayed data is only as current as the last time you collected from the remote machines.

Option	Description
Administration	View administrative details about the VCM Remote client. ■ To view the installed Remote client version, click **Administration** and select **Machines Manager > Licensed Machines > Licensed Windows Machines**. The Remote Client Version appears in the data grid. ■ To view the status of remote collection jobs, click **Administration** and select **Job Manager > History > VCM Remote**.

Tracking Unmanaged Hardware and Software Asset Data 15

VCM management extensions for assets integrates and manages hardware and software asset data that is not gathered through the automated managed machine collection processes of VCM.

- **Hardware**: VCM for assets stores supplemental information (data that is not automatically collected) about physical and virtual machines that are managed by VCM. In addition, VCM for assets stores data about non-managed enterprise equipment such as printers, mobile devices, routers, and so on.
- **Software**: VCM for assets can collect and store information about the software that is installed on physical and virtual machines managed by VCM.

VCM users view the asset data in the VCM Console, where, depending on assigned role, users might also have edit permission.

This chapter includes the following topics:

Configure Asset Data Fields 259
Configure Asset Data Values for VCM Machines 264
Configure Asset Data for Other Hardware Devices 264
Configure Asset Data for Software 267

Configure Asset Data Fields

An administrator must configure VCM for assets so that it includes the columns of data that apply to the hardware and software assets in your environment.

Procedure

1. "Review Available Asset Data Fields" on page 260

   VCM for assets is populated with a short list of data fields to get you started.

2. "Add an Asset Data Field" on page 260

   You can add any data that you want to store and manage about your hardware or software.

3. "Edit an Asset Data Field" on page 261

   Change VCM for assets data fields to keep up with your tracking and management needs for hardware or software.

4. "Delete a VCM for Assets Data Field" on page 262

   Remove asset data fields that do not serve a purpose in your environment.

5. "Change the Order of Asset Data Columns" on page 262

Changing the order of the VCM for assets data field list changes the order of columns when you view asset data in the VCM Console.

6. "Refresh Dynamic Asset Data Fields" on page 263

   You can force VCM for assets to refresh the values in all fields that are configured to populate dynamically.

Review Available Asset Data Fields

VCM for assets is populated with a short list of data fields to get you started. Examples include hardware data such as location or contact person, and software data such as license expiration date or number of copies.

VCM for assets is configurable, so review the data fields and the order in which they appear. You have the opportunity to add, modify, remove, and rearrange fields.

Prerequisites

- Log in to VCM using an account with the Administrator role.
- Identify the asset data that you want to store about your hardware or software.

Procedure

1. Click **Administration**.
2. Select **Settings > Asset Extensions Settings**.
3. Select one of the following nodes.

   Hardware Configuration Items > Other Devices
   Hardware Configuration Items > VCM Devices
   Software Configuration Items

4. In the data grid, review the names and descriptions.

   Each row, in order, becomes a column in the asset data display in the VCM Web Console.

What to do next

Supplement the populated data fields by adding more. See "Add an Asset Data Field" on page 260.

Add an Asset Data Field

You can add any data that you want to store and manage about your hardware or software.

Prerequisites

- Log in to VCM using an account with the Administrator role.
- Identify the asset data that you want to store about your hardware or software.

Procedure

1. Click **Administration**.
2. Select **Settings > Asset Extensions Settings**.
3. Select one of the following nodes.

   Hardware Configuration Items > Other Devices
   Hardware Configuration Items > VCM Devices
   Software Configuration Items

4. Click **Add**.
5. Type a name and description for the new asset data field and click **Next**.

   The name is the column heading that appears when users view the data in the VCM Console.
6. Specify properties about the new data.
   a. Select the way to populate the data.
      - **Manually**: type free-form text
      - **Lookup**: select from a fixed or query-based list of values
      - **Dynamically**: query from other data
   b. Select the data type.

      For string data, also enter the maximum number of characters to allow.
7. Click **Next**.
8. Configure the way to populate the data based on your earlier selection.
   - **Manually**: No configuration steps are needed. The user types the data at runtime.
   - **Lookup, fixed**: Create the fixed list by typing values and clicking **Add**. When finished, click **Next**.
   - **Lookup, query-based**: Type the SQL query that populates the list from which to select values, and click **Next**.
   - **Dynamic**: Type the SQL query that pulls the value from another data source, and click **Next**.
9. Select the roles that are allowed to edit the data.

   Only users assigned to these roles can edit the data using the VCM Console.
10. Review the settings and click **Finish**.

What to do next

Modify fields that need to be adapted for your site. See "Edit an Asset Data Field" on page 261.

Edit an Asset Data Field

Change VCM for assets data fields to keep up with your tracking and management needs for hardware or software.

Prerequisites

- Log in to VCM using an account with the Administrator role.
- Identify the asset data that you want to store about your hardware or software.

Procedure

1. Click **Administration**.
2. Select **Settings > Asset Extensions Settings**.
3. Select one of the following nodes.

   Hardware Configuration Items > Other Devices
   Hardware Configuration Items > VCM Devices
   Software Configuration Items
4. In the data grid, select the row.

5. Click **Edit**.
6. Change the name or description for the data field and click **Next**.

   The name is the column heading that appears when users view the data in the VCM Console.
7. Click **Next**.

   You cannot change the data properties.
8. Click **Next**.
9. Select the roles that are allowed to edit the data.

   Only users assigned to these roles can edit the data using the VCM Console.
10. Review the settings and click **Finish**.

What to do next

Remove unwanted fields. See "Delete a VCM for Assets Data Field" on page 262.

Delete a VCM for Assets Data Field

Remove asset data fields that do not serve a purpose in your environment.

Prerequisites

- Log in to VCM using an account with the Administrator role.
- Identify the asset data that you want to store about your hardware or software.

Procedure

1. Click **Administration**.
2. Select **Settings > Asset Extensions Settings**.
3. Select one of the following nodes.

   Hardware Configuration Items > Other Devices
   Hardware Configuration Items > VCM Devices
   Software Configuration Items
4. In the data grid, select the row.
5. Click **Delete**.

   You cannot delete entries that are marked with a lock icon.
6. Click **OK**.

What to do next

Rearrange asset data fields so that the order of columns shown in the VCM Console meets your requirements. See "Change the Order of Asset Data Columns" on page 262.

Change the Order of Asset Data Columns

Changing the order of the VCM for assets data field list changes the order of columns when you view asset data in the VCM Console.

Prerequisites

- Log in to VCM using an account with the Administrator role.
- Identify the asset data that you want to store about your hardware or software.

Procedure

1. Click **Administration**.
2. Select **Settings > Asset Extensions Settings**.
3. Select one of the following nodes.

   Hardware Configuration Items > Other Devices
   Hardware Configuration Items > VCM Devices
   Software Configuration Items

   In the data grid, each row, in order, becomes a column in the asset data display in the VCM Console.
4. Click **Column Order**.
5. Select entries, use the arrow buttons to move rows up or down, and click **Next**.
6. Review the rearranged order and click **Finish**.

What to do next

Refresh the values in dynamically generated fields. See "Refresh Dynamic Asset Data Fields" on page 263.

Refresh Dynamic Asset Data Fields

You can force VCM for assets to refresh the values in all fields that are configured to populate dynamically.

Prerequisites

Log in to VCM using an account with the Administrator role.

Procedure

1. Click **Administration**.
2. Select **Settings > Asset Extensions Settings**.
3. Select one of the following nodes.

   Hardware Configuration Items > Other Devices
   Hardware Configuration Items > VCM Devices
   Software Configuration Items
4. Click **Refresh Dynamic Fields**.

   The option recalculates and overwrites all dynamic data fields listed and might take time to finish.
5. Click **OK**.

What to do next

Enter data for machines that are managed by VCM. See "Configure Asset Data Values for VCM Machines" on page 264.

Configure Asset Data Values for VCM Machines

Although the asset data for machines that are managed by VCM is collected, you can customize some data through VCM for assets.

Prerequisites

Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Hardware Configuration Items > VCM Devices**.
3. In the data grid, select the VCM machine.
4. Click **Edit Values**.
5. Verify that the machine you want is in the Selected list and click **Next**.

   Use the arrow buttons to move entries to or from the Selected list.
6. Move the data fields that you want to edit into the Selected list and click **Next**.

   Use the arrow buttons to move entries to or from the Selected list.
7. Select or type the new values and click **Next**.
8. Review the new values and click **Finish**.

What to do next

Enter data for hardware that is not managed by VCM, such as printers, mobile devices, routers, and so on. See "Configure Asset Data for Other Hardware Devices" on page 264.

Configure Asset Data for Other Hardware Devices

A user with a role that has permission to edit asset data can populate VCM for assets with the hardware devices in your environment that are not discovered and managed by VCM.

Procedure

1. "Add Other Hardware Devices" on page 265

   Use VCM for assets to keep track of your non-VCM managed hardware by adding information about the hardware devices directly to VCM.
2. "Add Multiple Similar Other Hardware Devices" on page 265

   If your site has many nearly identical devices, you can use VCM for assets to clone one copy as a way to quickly add records for the other devices.
3. "Edit Asset Data for Other Hardware Devices" on page 265

   Use VCM for assets to change your hardware asset records as your enterprise changes.
4. "Edit Asset Data Values for Other Hardware Devices" on page 266

   You can change only the details about a given piece of equipment when the long term information, such as the model name or number, is going to remain the same.
5. "Delete Other Hardware Devices" on page 266

   Use VCM for assets to delete the records of hardware devices that are no longer a part of your site.

Add Other Hardware Devices

Use VCM for assets to keep track of your non-VCM managed hardware by adding information about the hardware devices directly to VCM.

Prerequisites

- Have an administrator configure the asset data fields that you need. See "Configure Asset Data Fields" on page 259.
- Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Hardware Configuration Items > Other Devices**.
3. Click **Add**.
4. Select or type the details that identify the device, such as its name and model, and click **Next**.
5. Select or type the values for the asset data associated with the device and click **Next**.

   The fields can vary depending on how the administrator configured your data for other hardware devices.
6. Click **Finish**.

Add Multiple Similar Other Hardware Devices

If your site has many nearly identical devices, you can use VCM for assets to clone one copy as a way to quickly add records for the other devices.

Prerequisites

- Log in to VCM with a role that has edit permission for asset configuration data.
- Create at least one copy of the device to serve as a baseline. See "Add Other Hardware Devices" on page 265.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Hardware Configuration Items > Other Devices**.
3. In the data grid, select the original, baseline asset.
4. Click **Clone**.
5. Modify the details to reflect the new copy of the asset and click **Next**.

   You must change at least the name.
6. Modify the values to reflect the asset data associated with the new device and click **Next**.
7. Click **Finish**.

Edit Asset Data for Other Hardware Devices

Use VCM for assets to change your hardware asset records as your enterprise changes.

Prerequisites

Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Hardware Configuration Items > Other Devices**.
3. In the data grid, select the asset.
4. Click **Edit**.
5. Change the details that identify the device, such as its name and model, and click **Next**.
6. Change the values for the asset data associated with the device and click **Next**.

   The fields can vary depending on how the administrator configured your data for other hardware devices.
7. Click **Finish**.

Edit Asset Data Values for Other Hardware Devices

You can change only the details about a given piece of equipment when the long term information, such as the model name or number, is going to remain the same.

Prerequisites

Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Hardware Configuration Items > Other Devices**.
3. In the data grid, select the asset.
4. Click **Edit Values**.
5. Move the data fields that you want to edit into the Selected list and click **Next**.

   Use the arrow buttons to move entries to or from the Selected list.
6. Select or type the new values and click **Next**.
7. Review the new values and click **Finish**.

Delete Other Hardware Devices

Use VCM for assets to delete the records of hardware devices that are no longer a part of your site.

Prerequisites

Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Hardware Configuration Items > Other Devices**.
3. In the data grid, select the asset.
4. Click **Delete**.
5. Click **OK**.

Configure Asset Data for Software

A user with a role that has permission to edit asset data can use VCM for assets to gather information about the software on machines that are discovered and managed by VCM.

Procedure

1. "Add Software Assets" on page 267

   Manage your software assets by having VCM for assets detect what is installed on the physical and virtual machines in your environment.

2. "Add Multiple Similar Software Assets" on page 268

   If your environment has many nearly identical copies of software, such as the same application with a different license number, you can use VCM for assets to clone one copy as a way to quickly add records for the others.

3. "Edit Asset Data for Software" on page 269

   Use VCM for assets to change your software asset records as your enterprise changes.

4. "Edit Asset Data Values for Software" on page 270

   You can change the details about a specific copy of software when the long term information, such as the application name or version, is going to remain the same.

5. "Delete Software Data" on page 270

   Use VCM for assets to delete entries for software that is no longer installed at your site.

Add Software Assets

Manage your software assets by having VCM for assets detect what is installed on the physical and virtual machines in your environment.

Prerequisites

- Have an administrator configure the asset data fields that you need. See "Configure Asset Data Fields" on page 259.
- Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Software Configuration Items**.
3. Click **Add Software**.
4. Type a name and description and click **Next**.
5. Select the data type that VCM for assets will look for to detect the installed software and click **Next**.

   The options take you to custom wizard pages where you type or select what VCM for assets will look for in the database.

   - **Software Inventory (Windows)**: Select a product from the software inventory (SI) list.
   - **Registry (Windows)**: Type or select a Windows Registry path, key, and value.
   - **File System - Known Files (Windows)**: Type or select a filename and version.
   - **Software Inventory - Packages (UNIX)**: Select a product from the SI list.
   - **Software Inventory - Utilities (UNIX)**: Select a product from the SI list.
   - **File System - Known Files (UNIX)**: Type or select a filename.
6. Click **Next**.
7. Select or type the values for the asset data associated with the software and click **Next**.

   The fields can vary depending on how the administrator configured your data for software.
8. Click **Finish**.

Add Multiple Similar Software Assets

If your environment has many nearly identical copies of software, such as the same application with a different license number, you can use VCM for assets to clone one copy as a way to quickly add records for the others.

Prerequisites

- Log in to VCM with a role that has edit permission for asset configuration data.
- Create at least one copy of the software to serve as a baseline. See "Add Software Assets" on page 267.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Software Configuration Items**.
3. In the data grid, select the original, baseline software asset.
4. Click **Clone**.
5. Modify the details to reflect the new copy of the software asset and click **Next**.

   You must change at least the name.

6. Change the data type that VCM for assets will look for to detect the installed software and click **Next**.

   The options take you to custom wizard pages where you type or select what VCM for assets will look for in the database.

   - **Software Inventory (Windows)**: Select a product from the software inventory (SI) list.
   - **Registry (Windows)**: Type or select a Windows Registry path, key, and value.
   - **File System - Known Files (Windows)**: Type or select a filename and version.
   - **Software Inventory - Packages (UNIX)**: Select a product from the SI list.
   - **Software Inventory - Utilities (UNIX)**: Select a product from the SI list.
   - **File System - Known Files (UNIX)**: Type or select a filename.
7. Click **Next**.
8. Modify the asset data values to reflect the new software and click **Next**.
9. Click **Finish**.

Edit Asset Data for Software

Use VCM for assets to change your software asset records as your enterprise changes.

Prerequisites

Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Software Configuration Items**.
3. In the data grid, select the software asset.
4. Click **Edit**.
5. Change the name or description and click **Next**.
6. Change the data type that VCM for assets will look for to detect the installed software and click **Next**.

   The options take you to custom wizard pages where you type or select what VCM for assets will look for in the database.

   - **Software Inventory (Windows)**: Select a product from the software inventory (SI) list.
   - **Registry (Windows)**: Type or select a Windows Registry path, key, and value.
   - **File System - Known Files (Windows)**: Type or select a filename and version.
   - **Software Inventory - Packages (UNIX)**: Select a product from the SI list.
   - **Software Inventory - Utilities (UNIX)**: Select a product from the SI list.
   - **File System - Known Files (UNIX)**: Type or select a filename.
7. Click **Next**.
8. Change the values for the asset data associated with the software and click **Next**.

   The fields can vary depending on how the administrator configured your data for software.
9. Click **Finish**.

Edit Asset Data Values for Software

You can change the details about a specific copy of software when the long term information, such as the application name or version, is going to remain the same.

Prerequisites

Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Software Configuration Items**.
3. In the data grid, select the software asset.
4. Click **Edit Values**.
5. Move the data fields that you want to edit into the Selected list and click **Next**.

   Use the arrow buttons to move entries to or from the Selected list.
6. Select or type the new values and click **Next**.
7. Review the new values and click **Finish**.

Delete Software Data

Use VCM for assets to delete entries for software that is no longer installed at your site.

Prerequisites

Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Software Configuration Items**.
3. In the data grid, select the software asset.
4. Click **Delete**.
5. Click **OK**.

Managing Changes with Service Desk Integration 16

VCM Service Desk Integration tracks planned and unplanned changes to managed machines in your organization, and integrates change requests with your change management process.

Service Desk Integration works by temporarily holding requested changes to managed machines while VCM integrates with your service desk application in order to pass the requests through your change management process or workflow. After the changes are approved, VCM resumes changing the managed machines, in order of criticality.

VCM Service Desk Connector links VCM with the service desk application in order to track and manage the VCM initiated changes. Change management process and workflow definitions vary by customer and depend on the configuration implemented during your VMware services engagement.

This chapter includes the following topics:

Configure Service Desk Integration 271

View Service Desk Integration in the Console 271

View Service Desk Integration in Job Manager 272

Configure Service Desk Integration

To add the Service Desk Integration feature to VCM, you must complete the following high-level tasks.

Procedure

1. Contact VMware Customer Support to determine the requirements for your integration and arrange for a VMware services engagement.
2. License Service Desk Integration.
3. Activate Service Desk Integration

After VMware Customer Support assists you with licensing and the integration of VCM with your service desk application, additional nodes that are unique to the service desk feature appear in VCM.

What to do next

Look at your service desk data. See "View Service Desk Integration in the Console" on page 271.

View Service Desk Integration in the Console

When service desk integration is enabled, the Service Desk data grids provide a detailed view of VCM-related service desk events.

Procedure

1. Click **Console**.
2. Select **Service Desk**.
3. Under the Service Desk node, select any subnode.

   For example, click **By RFC** to view the data according to request for change (RFC). Under the By RFC sub-node, select an RFC to view the data for that item.

Your subnodes and data views might differ from the defaults or from other organizations based on your requirements and specific implementation.

What to do next

Look at the status of change jobs. See "View Service Desk Integration in Job Manager" on page 272.

View Service Desk Integration in Job Manager

VCM Service Desk Integration pauses requested changes to managed machines while VCM integrates with your service desk application to pass the request through your change management process.

Procedure

1. Click **Administration**.
2. Select **Job Manager > Pending Response**.

   After the job is approved, it is released to run immediately or at a scheduled time.
3. Select **Job Manager > Running**.

   Alternately, select **Job Manager > Scheduled**.

NOTE Patching jobs are in a different location. Locate patching jobs by clicking **Patching** and selecting **VCM Patching Administration** > *operating-system* > **Job Manager**.

Index

A

about this book **9**
access
  by user **11**
  compliance content **21**
active directory
  collection results **242**
  configuration **239**
  data collection **242**
  getting started **233**
  install **240**
  run determine forest action **240**
  run domain controller setup action **241**
add servers
  provisoning, operating system **202**
adding
  asset data field **260**
  hardware asset data **265**
  Linux machines **124**
  Mac OS X machines **124**
  multiple hardware asset data **265**
  multiple software asset data **268**
  repository sources **227**
  service desk integration **271**
  software asset data **267**
  UNIX machines **124**
  vCenter Server **30**
  vCloud Director **37**
  vShield Manager **47**
administration settings
  configuring for patching **173**
administrator privileges for patching **138**
agent
  install, Windows **91**
  installation
    Linux agent, enable **123**
    UNIX agent, enable **123**
  installation, Linux **117**
  installation, Mac OS X **117**
  installation, UNIX **117**
  remote client **248**
agent communication
  changing after OS provisioning **213**
agent installation parameters
  Linux **127**
  Mac OS X **127**
  UNIX **127**
agent proxy
  collector **51**
AIX machines
  patching **141**
alerts
  compliance
    machine groups **192-193**
alternate locations
  configuring **161**
  Red Hat Linux machine **169**
alternative location patch repository **139**
assessment
  SCAP **195-196**
assessment results
  Linux and UNIX patching **147**
  manual patching for Windows **154**
assessment templates for patching **142**
assessments
  manual patching for Windows **153**
assets
  adding data field **260**
  adding hardware data **265**
  adding multiple hardware data **265**
  adding multiple software data **268**
  adding software data **267**
  configuring data fields **259**
  configuring hardware data **264**
  configuring software data **267**
  deleting data field **262**
  deleting hardware data **266**
  deleting software data **270**
  editing hardware data **265**
  editing hardware data values **266**
  editing software data **269**
  editing software data values **270**
  edting data field **261**
  getting started **259**
  rearranging data fields **262**
  refreshing dynamic data field **263**
  reviewing data field **260**
  VCM asset data **264**
assigning
  network authority account **89**
auditing **85**
automated patching
  deployment mapping **175**
  environment **156**
  trigger events **169**
  troubleshooting **138**, **140**
automatic patch deployment
  configuring settings **174**
  job chain **158**, **170-171**, **176**
  patching exceptions **172**

availble domains
domain controllers **234**

B

badge score
vCenter Operations Manager **74**, **76-80**
base path of SCR Tool **168**
bulletin details
manual patching for Windows **152**
bulletin updates
manual patching for Linux and UNIX **144**
manual patching for Windows **151**
bulletins
dynamic membership **171**

C

certificates
remote client **246**
change
vCenter Operations Manager **73**
change management
WCI **107**
checking
network authority account **89**, **234**
collect
domain controllers **238**
ESX logs **50**, **55**
ESX service console operating system **50**
hosts, virtual machine **52**
installation delegate **121**
Linux, UNIX, and Mac OS X data **132**
package managers **225**
repositories **226**
schedule Linux, UNIX, and Mac OS X **135**
vCenter Server **32**
vCenter Server virtual machines **35**
vCloud Director **37**, **39**
vCloud Director vApp **41**
virtual machine hosts **52**
vShield Manager **47**, **49**
WCI data **108**
collect distributions
provisioning, operating system **203**
collection filter for WCI **111**
collection filters
Linux and UNIX patching **145**
collection results
active directory **242**
Linux, UNIX, and Mac OS X **133**
Remote **256**
WCI **113**
collection scripts
custom for WCI **109**
collections
active directory **242**
domain controllers **238**
manual patching for Windows **153**
vCenter Server data **29**, **33**
virtualization **55**
WCI **110**
Windows machines **94**
collections for Windows patch assessments **138**
collector
agent proxy **51**
aware of Remote client **246**, **256**
compliance
content, access **21**
machine groups **181**
alerts **192**
alerts, add **192**
alerts, configure **193**
download content **182**
filters, add **185**
resolve noncompliant results **189**
resolve noncompliant results, enforceable **189**
resolve noncompliant results, exceptions **191**
resolve noncompliant results, manually **67**, **191**
resolve noncompliant results, VCM actions **66**, **190**
rule groups, add **184**
rule groups, preview **186**
rules, add **184**
schedule **192**
schedule, add **194**
templates **187**
templates, run **188**
software provisioning **230-231**
templates
machine groups **182**
virtual environments
resolve noncomplaint results, exceptions **191**
resolve noncomplaint results, manually **67**, **191**
resolve noncomplaint results, VCM actions **66**, **190**
compliance exceptions
vCenter Server **65**, **67**, **191**
vCloud Director **65**, **67**, **191**
virtual objects **65**, **67**, **191**
compliance filters
vCenter Server **62**
vCloud Director **62**
virtual objects **62**
compliance rule groups
preview **62**
vCenter Server **60**
vCloud Director **60**
virtual objects **60**
compliance rules
vCenter Server **61**
vCloud Director **61**
virtual objects **61**
compliance templates
vCenter Server **59**, **63**
vCloud Director **59**, **63**
virtual objects **59**, **63**

configuration
Active Directory **239**
configuration of patch staging **163**
configure
SCR Tool **160**
configuring
alternate location machines **161**
asset data field **259**
event-driven patch assessment **170**
event-driven patch deployment **170**
hardware data **264**
machine group mapping **167**
managed machines patch staging **165**
patching administration settings **173**
patching repository **144**, **158**
protocols for patch staging **159**
scheduled patch assess and deploy **176**
software data **267**
VCM with alternate locations **162-163**
VCM with patching repository **162-163**
vSphere Client Plug-in **57**
console
service desk integration **271**
content
compliance **21**
content for compliance
wizard **20**
copying
files to ESX/vSphere servers **54**
create packages
software provisioning **223**
custom filter sets
remote **247**
remote client **248**
customization
for your environment **16**

D

data age
deploy patches **174**
deleting
asset data field **262**
hardware asset data **266**
software asset data **270**
deploying patches
applicability changes **174**
group membership changes **174**
how it works **178**
Linux and UNIX patching **148**
manual patching for Windows **155**
no run level change **140**
Solaris, single-user mode **140**
template membership changes **174**
threshold data age **174**
wizards **179**
determine forest action
running for active directory **240**
develop
custom collection scripts **109**
discover
domain controllers **235**
vCloud Director vApp **43**
discovering
domain controllers **233**, **235**
Windows machines **87**, **90**
discovery
provisioning, operating system **203**
distributed patching
protocols **159**
Red Hat Linux machines **169**
domain
active directory **233**
domain controllers
add network authority **234**
assign network authority **235**
available domains **234**
collect **238**
collecting **238**
discover **235**
discover, license, install **233**
discovering **235**
domain discovery **234**
license **236**
licensing **236**
run setup action **241**
domain discovery
domain controllers **234**
Windows machines **88**
download
SCR Tool **159**
download patches
manual patching for Windows **152**
dynamic membership for patch bulletins **171**
dynamic patch assessment templates **171**

E

editing
asset data field **261**
hardware asset data **265**
hardware asset data values **266**
software asset data **269**
software asset data values **270**
VCM asset data **264**
enabling
instsallation delgate **123**
patching repository **164**
patching repository trust status **164**
environment
automated patching **156**
ESX
collect **52**
service console operating system collection **50**
ESX files
copy **54**
ESX logs
collect **50**, **55**
event-driven patch deployment **169**
assessment template **171**

exploring
Remote collection results **256**
exporting
SCAP assessment **197**
F
filter for WCI collections **111**
filter sets
remote **247**
remove client **247**
forest
active directory **233**
run determine forest action **240**
foundation checker **19**
installation **22**
G
getting started
active directory **233**
assets **259**
auditing **85**
launching **12**
logging on **12**
manual patch deployment for Linux and UNIX **148**
manual patching **143**
remote client **245**
tools **19**
virtualization **23**
vSphere Client Plug-in **58**
WCI **95**
WCI PowerShell scripts **97**
group membership changes
deploy patches **174**
H
host files
remote client **248**
hosts
collect **52**
how it works
job chain for Linux and UNIX **178**
patch deploy action **178**
patch staging for Linux and UNIX **177**
HTTPS bypass
Linux agent installation **123**
I
import/export wizard **20**
importing
SCAP benchmark **195**
information bar
portal **13**
installation
foundation checker **22**
tools **19**
Windows machines **87**, **233**
installation delegate **118**, **121**
collect **121**
enable **123**
trust status **122**
installing
agent, Linux **125**
agent, Mac OS X **125**
Package Studio **220**
packages **228**
PowerShell **110**
remote client **250-251**, **253**
repositories **219**
software provisioning **218**
UNIX agent **125**
VCM for active directory **240**
installing package manager
software provisioning **222**
installing package studio
software provisioning **220**
installing repository
software provisioning **219**
integration
service desk **271**
J
JCE on patching repository **160**
job chain
automated patching **158**, **170-171**, **176**
how it works **178**
job manager **19**
service desk integration **272**
job status reporting
WCI **112**
jobs
time out for patching **170**, **179**
jobs history
provisioning **230**
JRE on patching repository **160**
L
license
domain controllers **236**
licensing
domain controllers **233**, **236**
Windows machines **87**, **91**
Linux
add machines **124**
agent installation **117**
agent installation parameters **127**
collect data **132**
collecting
schedule **135**
scheduled collection **133**
collection results **133**
installing agent **125**
machine group, create **134**
Linux agent
enable installation **123**
Linux and UNIX
assessment results for manual patching **147**
manual bulletin updates **144**
manual patch assess and deploy **141**
manual patch collection **145**
patch collection filters **145**

patch deployment **148**
patching getting started **143**
running patching reports **180**
Linux and UNIX patch staging **177**
Linux and UNIX patching job chain **178**
logs
ESX **56**

M

Mac OS X
add machines **124**
agent installation **117**
collect data **132**
collecting
schedule **135**
scheduled collection **133**
collection results **133**
installing agent **125**
machine group, create **134**
Mac OS X agent
enable installation **123**
machine group mapping **163**
configuring for patching **167**
machine groups
compliance **181**
alerts **192**
alerts, add **192**
alerts, configure **193**
download content **182**
filters **185**
resolve noncompliant results **189**
resolve noncompliant results, enforceable **189**
resolve noncompliant results, exceptions **191**
resolve noncompliant results, manually **67**, **191**
resolve noncompliant results, VCM actions **66**, **190**
rule groups preview **186**
rule groups, add **184**
rules, add **184**
schedule **192**
schedule, add **194**
templates, add **187**
templates, run **188**
compliance templates **182**
create
Linux, UNIX, and Mac OS X **134**
manage patching repository **139**
managed machines
adding patching exceptions **172**
configure patch staging **165**
patch assessment **172**
patching **137**
managing agent
virtual environments **26**
managing agent collection
virtual environments **26**
managing agent enabled
virtual environments **28**
managing agent HTTPS bypass
virtual environments **28**
managing agent trust status
virtual environments **27**
managing agent;SSL thumbprint **29**
manual patch assess and deploy **141**
manual patching
download Windows patches **152**
filters for Linux and UNIX **145**
getting started **143**
Linux and UNIX assessment results **147**
Linux and UNIX bulletin updates **144**
Linux and UNIX collection **145**
Linux and UNIX patch deployment **148**
troubleshooting **138**, **140**
Windows assessment results **154**
Windows assessments **153**
Windows bulletin details **152**
Windows bulletin updates **151**
Windows collections **153**
Windows deployment **155**
mapping
create **76**
dashboard **78**
schedule **78**
vCenter Operations Manager **73-74**, **77-80**
mapping for patch deployment **175**

N

NAT
see network address translation **41**
navigation sliders **15**
network address translation
vCloud Director vApp **41**
network authority
add **234**
assign **235**
network authority account
assigning **89**
checking **89**, **234**

O

operating system
virtual machine **36**
operating system provisioning **199**
overview
SCAP **194**
vSphere Client Plug-in **56**

P

package
installing **228**
package manager
collect **225**
Package Studio
installing **220**
patch assessments
collections for Windows **138**

patch staging
configuring for managed machines **165**
how it works **177**
Linux and UNIX **177**
patches
SCR Tool **159**
patching **172**
administrator privileges **138**
AIX machines **141**
alternate location **139**
applicability of patches for deployment **174**
assessment and deployment **137**
assessment templates **142**
assessments for Windows **153**
bulletin details for Windows **152**
bulletins dynamic membership **171**
collections for Windows assessments **153**
configuring event-driven assessments **170**
configuring event-driven deployment **170**
configuring machine group mapping **167**
deployment mapping **175**
deployment wizards **179**
distributed model **169**
event-driven deployment **169**
exceptions **171-172**
how patch deployment works **178**
how the job chain works **178**
JCE on patching repository **160**
job chain **158**, **170-171**, **176**
jobs time out **170**, **179**
JRE on patching repository **160**
Linux and UNIX assessment results **147**
Linux and UNIX collection filters **145**
Linux and UNIX deployment **148**
Linux and UNIX getting started **143**
Linux and UNIX job chain **178**
machine group mapping **163**
managed machines **137**
manual assess and deploy **141**
manual assessment results for Windows **154**
manual bulletin updates for Windows **151**
manual deployment for Windows **155**
manual Linux and UNIX collection **145**
manual patch download for Windows **152**
manual updates for Linux and UNIX **144**
no change in run level **140**
patch staging configuration **163**
prerequisites **137-138**
reports **180**
requirements **138**
runtime properties files **160**
scheduled assessments **176**
scheduled deployment **170**
Solaris, single-user mode **140**
supported managed machines **137**
Windows getting started **150**
patching repository **144**, **158**
enable trust and status **164**
management **139**
Red Hat Linux machine **169**
SCR Tool base path **168**
portal
familiarizing **13**
information bar **13**
navigation sliders **15**
toolbar **14**
PowerShell
example script **102**
executing for WCI **102**
installation **110**
references **102**
script signing policies **101**
scripts, troubleshooting **115**
signing scripts for WCI **102**
WCI getting started **97**
Windows Custom Information **110**
PowerShell script
verifying **109**
prerequisites
patching deployment **137**
prerequisites for patching **138**
preview
compliance rule groups **62**
properties files **160**
protocols
configure for Linux and UNIX patching **159**
provision machines
operating systems **204**, **208**
provisioning
compliance **231**
compliance rule **230**
jobs History **230**
provisioning, operating system **199**
add servers **202**
agent communication **213**
collect distributions **203**
components **199**
discovery **203**
provision machines **204**, **208**
re-provision machines **214**
results **213**
servers **201**
set server trust status **202**
time, Linux **212**
workflow **200**
provisioning, software **217**, **225**
create packages **223**
install package manager **222**
install package studio **220**
install repository **219**
installation **218**
purge
for WCI **111**

R

re-provisioning machines
operating systems **214**

rearranging
asset data fields **262**
Red Hat Linux machines for patching **169**
refreshing
dynamic asset data field **263**
registering
vSphere Client Plug-in **56**
remediation
compliance rule **231**
remote
collection results **256**
filter sets **247**
settings **246**
remote client
certificates **246**
collector aware **246**, **256**
configure VCM remote **245**
getting started **245**
installation **249**
installation, command line **251**
installation, manual **250**
installation, remote commands **253**
network **256**
settings **246**
settings, custom filter sets **248**
settings, filter sets **247**
settings, host files **248**
reports
patching **180**
WCI **114**
repository
collect software **226**
installing software **219**
repository sources
adding **227**
requirements for patching **138**
results
collection, active directory **242**
ESX logs **56**
provisioning, operating system **213**
SCAP **196**
vCloud Director **40**
virtualization **56**
vShield Manager **50**
reviewing
asset data field **260**
run compliance
vCenter Server **64**
vCloud Director **64**
virtual objects **64**
running
determine forest action **240**
domain controller setup **241**
patching reports **180**
runtime properties files for patching **160**

S

SCAP
assessment **195-197**
benchmark **195**
exporting assessment **197**
importing benchmark **195**
overview **194**
results **196**
schedule
collection
Linux, UNIX, and Mac OS X **133**
compliance
machine groups **192-194**
scheduled patch assess and deploy **176**
scheduled patch deployment **170**
score
vCenter Operations Manager **73-74**, **76-80**
SCR Tool
configuration **160**
SCR Tool base path **168**
script
PowerShell **97**
PowerShell example **102**
verify validity **109**
script-based collection filter **111**
script signing
policies **101**
references **102**
service desk integration **271**
adding **271**
console **271**
job manager **272**
set server trust status
provisoning, operating system **202**
settings
remote **246**
vCloud Director **38**
vShield Manager **48**
setup action **241**
signing
policies, PowerShell scripts **101**
PowerShell scripts **102**
single-user mode **138**
sliders
in portal **15**
Software Content Repository (SCR) Tool **159-160**
software provisioning **217**, **225**
create packages **223**
install package manager **222**
install package studio **220**
install repository **219**
installation **218**
Solaris single-user mode patching **140**
sources
repository sources **227**
SSL thumbprint
managing agent **29**
staging patches **162**
configure protocols **159**
standards compliance
create **76**
dashboard **78**

run **77**
schedule **78**
vCenter Operations Manager **73-74**, **76-80**

T

template
deploy patches, membership changes **174**
patch assessment **142**
threshold data age
deploy patches **174**
time
provisioning, Linux operating system
Linux **212**
time-out
patching jobs **170**, **179**
ToCMBase64String **98**
toolbar
in portal **14**
tools
foundation checker **19**
getting started **19**
import/export, content **19**
installation **19**
job manager **19**
trigger events for automated patching **169**
troubleshooting
patching **138**, **140**
PowerShell scripts **115**
trust
enable for patching repository **164**
trust status
installation delegate **122**

U

UNIX
add machines **124**
agent installation **117**
agent installation parameters **127**
collect data **132**
collecting
schedule **135**
scheduled collection **133**
collection results **133**
installing agent **125**
machine group, create **134**
UNIX agent
enable installation **123**
UNIX and Linux
manual patch collection **145**
patch collection filters **145**
patching getting started **143**, **150**
user access **11**

V

vCenter Operations Manager **73**
badge score **74**, **76-80**
change **73**
compliance standards **73**
mapping **73-74**, **77-80**
vCenter Server **23**
add **30**
collect **32**
compliance exceptions **65**, **67**, **191**
compliance filters **62**
compliance rule groups **60**
compliance rules **61**
compliance templates **59**, **63**
data collections **29**
run compliance **64**
vCenter Server virtual machines
collect **35**
vCloud Director
add **37**
collect **37**, **39**
collection results **40**
compliance exceptions **65**, **67**, **191**
compliance filters **62**
compliance rule groups **60**
compliance rules **61**
compliance templates **59**, **63**
run compliance **64**, **188**
settings **38**
vApp collection **41**
vApp network address translation **41**
vCloud Director vApp
discover **43**
VCM asset data
editing **264**
verify PowerShell script **109**
virtual environment
collecting
results **56**
collections **55**
compliance
resolve noncompliant results **189**
resolve noncompliant results, exceptions **191**
resolve noncompliant results, manually **67**, **191**
resolve noncompliant results, VCM actions **66**, **190**
getting started **23**
managing agent **26**, **29**
managing agent collection **26**
managing agent enabled **28**
managing agent HTTPS bypass **28**
managing agent trust status **27**
virtual machine
manage operating system **36**
vCloud Director vApp **41**
virtual object
compliance exceptions **65**, **67**, **191**
compliance filters **62**
compliance rule groups **60**
compliance rules **61**
compliance templates **59**, **63**
run compliance **64**
vShield Manager
add **47**
collect **47**, **49**

collection
results **50**
settings **48**
vSphere Client Plug-in
configuring **57**
getting started **58**
overview **56**
registering **56**

W

WCI
challenges CDATA **101**
challenges in column names **100**
challenges in scripting **98**
challenges in task entries **100**
change management **107**
collecting data **108**
collection **110**
collection filter **111**
collection results **113**
custom collection scripts **109**
executing PowerShell scripts **102**
getting started **95**
guidelines in scripting **98**
job status reporting **112**
prerequisites to collect **96**
purge **111**
running reports **114**
verify PowerShell script **109**
Windows
assessments for patching **153**
bulletin details for patching **152**
collections for patching **153**
manual assessment results **154**
manual bulletin updates **151**
manual deployment **155**
manual patch assess and deploy **141**
manual patch download **152**
patching getting started **150**
running patching reports **180**
Windows Custom Information (WCI) **95**
Windows machine
collecting **94**
discover, license, install **87**
discovering **90**
domain discovery **88**
licensing **91**
wizards
content **20**
import/export **20**